



NB504

54Mbps Wireless Router

CONTENTS

Package Contents	4
Chapter 1: About this Guide	5
1.1 Purposes	5
1.2 Conventions	5
1.3 Overview of this User Guide	5
Chapter 2: Introduction	6
2.1 Overview of the Router	6
2.2 Features	7
2.3 Panel Layout	8
2.3.1 The Front Panel	8
2.3.2 The Rear Panel	9
Chapter 3: Connecting the Router	10
3.1 System Requirements	10
3.2 Installation Environment Requirements	10
3.3 Connecting the Router	11
Chapter 4: Quick Installation Guide	12
4.1 TCP/IP configuration	12
4.2 Quick Installation Guide	14
Chapter 5: Configuring the Router	19
5.1 login	19
5.2 Status	20
5.3 Quick Setup	22
5.4 Network	22
5.4.1 LAN	22
5.4.2 WAN	23
5.4.3 MAC Clone	33
5.5 Wireless	34
5.5.1 Wireless Settings	35
5.5.2 MAC Filtering	38
5.5.3 Wireless Statistics	41
5.6 DHCP	42
5.6.1 DHCP Settings	43
5.6.2 DHCP Clients List	44
5.6.3 Address Reservation	45

5.7 Forwarding.....	47
5.7.1 Virtual Servers	47
5.7.2 Port Triggering	49
5.7.3 DMZ	51
5.7.4 UPnP	52
5.8 Security	53
5.8.1 Firewall	54
5.8.2 IP Address Filtering	55
5.8.3 Domain Filtering	57
5.8.4 MAC Filtering.....	59
5.8.5 Remote Management.....	61
5.8.6 Advanced Security	62
5.9 IP & MAC Binding Settings.....	64
5.9.1 Binding Setting	64
5.9.2 ARP List	66
5.10 Static Routing.....	67
5.11 Dynamic DDNS.....	68
5.11.1Dyndns.org DDNS	68
5.11.2 Oray.net DDNS	69
5.11.3 Comexe.cn DDNS	70
5.12 System Tools.....	71
5.12.1 Time	72
5.12.2 Firmware.....	73
5.12.3 Factory Defaults.....	74
5.12.4 Backup and Restore.....	74
5.12.5 Reboot	75
5.12.6 Password	75
5.12.7 Log.....	76
5.12.8 Statistics	77
Appendix A: FAQ.....	78
Appendix B: Configuring the PC.....	83
Appendix C: Specifications	88
Appendix D: Glossary.....	89
Appendix E: Legal and Regulatory Information.....	90

PACKAGE CONTENTS

The following contents should be found in your box:

- One NB504 54Mbps Wireless Router
- One AC power Adapter for NB504 54Mbps Wireless Router
- Quick Installation Guide
- One Resource CD for NB504 54Mbps Wireless Router, including:
 - This Guide
 - Other Helpful Information

Note: If any of the listed contents are damaged or missing, please contact the retailer from whom you purchased the NB504 54Mbps Wireless Router for assistance.

CHAPTER 1: ABOUT THIS GUIDE

Thank you for choosing the NB504 54Mbps Wireless Router. This router provides dedicated solution for Small Office/Home Office (SOHO) networks. With your network all connected, your local wired or wireless network can share Internet access, files and fun for multiple PCs through one ISP account.

It is an easy web-based setup for installation and management. Even though you may not be familiar with the router, this guide will make configuring the router easy. Before installing the router, please look through this guide to get to know all the router's functions.

1.1 Purposes

This Guide tells you how to use the NB504 54Mbps Wireless Router.

1.2 Conventions

The router mentioned in this guide stands for NB504 54Mbps Wireless Router.

1.3 Overview of this User Guide

Chapter 1: About this Guide

Chapter 2: Introduction

Chapter 3: Connecting the Router

Chapter 4: Quick Installation Guide

Chapter 5: Configuring the Router

Appendix A: FAQ

Appendix B: Configuring the PC

Appendix C: Specifications

Appendix D: Glossary

Appendix E: Contact Information

CHAPTER 2: INTRODUCTION

2.1 Overview of the Router

The NB504 54Mbps Wireless Router integrates 4-port Switch, firewall, NAT-router and Wireless AP. Its design is dedicated to Small Office/Home Office (SOHO) wireless network solutions. The NB504 54Mbps Wireless Router will allow you to connect your network wirelessly better than ever, sharing Internet Access, files and fun, easily and securely.

In the most attentive wireless security, the NB504 54Mbps Wireless Router provides multiple protection measures. It can be set to turn off wireless network name (SSID) broadcast so that only stations that have the SSID can be connected. The router provides wireless LAN 64/128/152-bit WEP encryption security, and WPA/WPA2 and WPA-PSK/WPA2-PSK authentication, as well as TKIP/AES encryption security. It also supports VPN pass-through for sensitive data secure transmission.

The NB504 54Mbps Wireless Router complies with the IEEE 802.11g/b standards so that the data transmission rate is up to 54Mbps. It is compatible with all IEEE 802.11g and IEEE 802.11b products.

The NB504 54Mbps Wireless Router provides flexible access control so that parents or network administrators can establish restricted access policies for children or staff. It has built-in NAT and DHCP server supporting static IP address distributing. It also supports Virtual Server and DMZ host for Port Triggering needs, and remote management and log so that network administrators can manage and monitor the network in real time.

The NB504 54Mbps Wireless Router is easy-to-manage. Quick Setup is supported and friendly help messages are provided for every step. So you can configure it quickly and share Internet access, files and fun.

2.2 Features

- Complies with IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 802.3u standards.
- 1 10/100M Auto-Negotiation RJ45 WAN port, 4 10/100M Auto-Negotiation RJ45 LAN ports, supporting Auto MDI/MDIX.
- Supports 54/48/36/24/18/12/9/6Mbps or 11/5.5/3/2/1Mbps data transfer rates.
- Provides WPA/WPA2, WPA-PSK/WPA2-PSK authentication, TKIP/AES encryption security.
- Shares data and Internet access for users, supporting PPPoE, Dynamic IP, Static IP, L2TP, PPTP, BigPond Cable Internet access.
- Supports Virtual Server, Special Application and DMZ host.
- Supports UPnP, Dynamic DNS, Static Routing, VPN Pass-through.
- Connecting Internet on demand and disconnecting from the Internet when idle for PPPoE.
- Built-in NAT and DHCP server supporting static IP address distributing.
- Built-in firewall supporting IP address filtering, Domain Name filtering, and MAC address filtering.
- Supports connecting/disconnecting from the Internet on a specified time of day.
- Supports access control, parents and network administrators can establish restricted access policies based on time of day for children or staff.
- Provides 64/128/152-bit WEP encryption security and wireless LAN ACL (Access Control List).
- Supports Flow Statistics.
- Supports ICMP-FLOOD, UDP-FLOOD, TCP-SYN-FLOOD filter.
- Ignores Ping packets from WAN or LAN ports.
- Supports firmware upgrade.
- Supports Web management.

2.3 Panel Layout

2.3.1 The Front Panel

The front panel of the NB504 consists of several LED indicators, which is designed to indicate connections. View from left. Table 2-1 describes the LEDs on the front panel of the router.



Figure 2-1 Front Panel

Name	Action	Description
POWER	Not lit	No Power
	Lit up	Power on
SYSTEM	Lit up	The router is initializing
	Flashing	The router is working properly
WLAN	Not lit	The router has a hardware error
	Not lit	There is no wireless device linked to the device
	Flashing	The Wireless function is enabled
WAN,1-4	Not lit	There is no device linked to the corresponding port
	Lit up	There is a device linked to the corresponding port but no activity
	Flashing	There is an active device linked to the corresponding port

Table 2-1 The LEDs description

2.3.2 The Rear Panel

The rear panel contains the following features. (View from left to right:)

- AC power socket: only use the power adapter supplied with the NB504 54Mbps Wireless Router, use of a different adapter may result in product damage.
- Four 10/100Mbps RJ45 LAN ports for connecting the router to the local PCs
- RJ45 WAN port for connecting the router to a cable, DSL modem, or Ethernet
- Factory Default Reset button
- There are two ways to reset the router's factory defaults:
 - 1) Use the **Factory Defaults** function on **System Tools** -> **Factory Defaults** page in the router's Web-based Utility.
 - 2) Use the Factory Default Reset button: First, turn off the router's power. Second, press and hold the default reset button then turn on the router's power, until the System LED lights up (about 3 seconds). Last, release the reset button and wait for the router to reboot.

Note: Ensure the router is powered on before it restarts completely.

- Wireless antenna

CHAPTER 3: CONNECTING THE ROUTER

3.1 System Requirements

- Broadband Internet Access Service (DSL/Cable/Ethernet)
- One DSL/Cable modem that has an RJ45 connector
- Each PC in the LAN needs a working Ethernet Adapter and an Ethernet cable with RJ45 connectors
- TCP/IP protocol must be installed on each PC
- Web browser, such as Microsoft Internet Explorer 5.0 or later, Netscape Navigator 6.0 or later

3.2 Installation Environment Requirements

- Do not place in direct sunlight or near a heater or heating vent
- Do not cluttered or crowded. There should be at least 2 inches (5 cm) of clear space on all sides of the router
- Well ventilated (especially if it is in a closet)
- Operating temperature: 0°C~40°C (32°F~104°F)
- Operating Humidity: 10%~90%RH, Non-condensing

3.3 Connecting the Router

Before you install the router, you should connect your PC to the Internet through your broadband service successfully. If there is any problem, please contact your ISP. After that, please install the router according to the following steps. Don't forget to pull out the power plug and keep your hands dry.

1. Power off your PC, Cable/DSL modem, and the router.
2. Locate an optimum location for the router. The best place is usually near the center of the area in which your PC will wirelessly connect. The place must accord with the Installation Environment Requirements.
3. Adjust the direction of the antenna. Normally, upright is a good direction.
4. Connect the PCs and each Switch/Hub in your LAN to the LAN Ports on the router. (If you have the wireless NIC and want to use wireless connector, you can skip this step.)
5. Connect the DSL/Cable Modem to the WAN port on the router.
6. Connect the AC power adapter to the AC power socket on the router, and the other end into an electrical outlet. The router will start to work automatically.
7. Power on your PC and Cable/DSL modem.

CHAPTER 4: QUICK INSTALLATION GUIDE

After connecting the NB504 Router into your network, you should configure it. This chapter describes how to configure the basic functions of your NB504 Wireless Router. These procedures only take you a few minutes. You can access the Internet via the router immediately after successfully configuring.

4.1 TCP/IP configuration

The default IP address of the NB504 54Mbps Wireless Router is 192.168.1.1. And the default Subnet Mask is 255.255.255.0. These values can be seen from the LAN. They can be changed as you desire, as an example we use the default values for description in this guide.

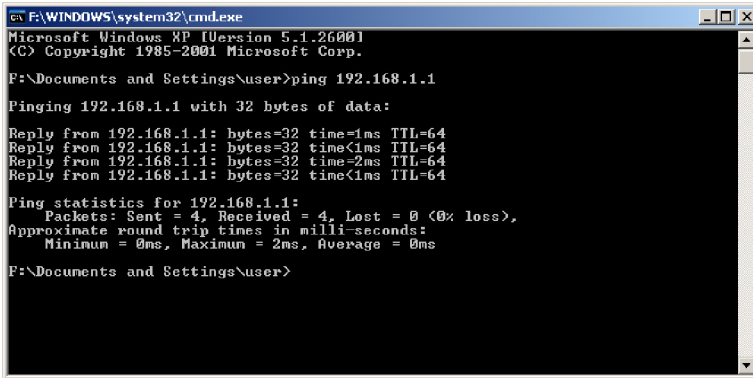
Connect the local PC to the LAN ports of the router, with an RJ45 cable (not supplied). There are then two ways to configure the IP address for your PC.

- Configure the IP address manually
 - 1) Set up the TCP/IP Protocol for your PC. If you need instructions as to how to do this, please refer to **Appendix B: “Configuring the PC.”**
 - 2) Configure the network parameters. The IP address is 192.168.1.xxx (“xxx” is from 2 to 254), Subnet Mask is 255.255.255.0, and Gateway is 192.168.1.1 (The router’s default IP address)
- Obtain an IP address automatically
 - 1) Set up the TCP/IP Protocol in **“Obtain an IP address automatically”** mode on your PC. If you need instructions as to how to do this, please refer to Appendix B: “Configuring the PC.”
 - 2) Power off the router and PC. Then turn on the router and restart the PC. The built-in DHCP server will assign IP address for the PC.

Now, you can run the Ping command in the **command prompt** to verify the network connection between your PC and the router. The following example is in Windows 2000 OS.

Open a command prompt, and type ping 192.168.1.1, then press Enter.

If the result displayed is similar to that shown in figure 4-1, the connection between your PC and the router has been established.



```

C:\F:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

F:\Documents and Settings\User>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

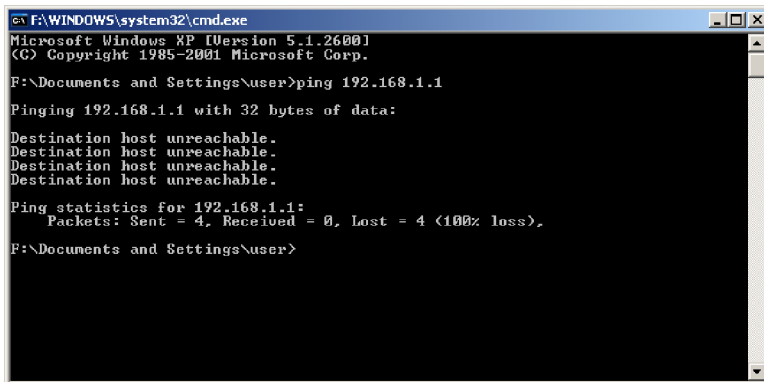
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms

F:\Documents and Settings\User>
```

Figure 4-1 Successful result of Ping command

If the result displayed is similar to that shown in figure 4-2, it means that your PC has not connected to the router.



```

C:\F:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

F:\Documents and Settings\User>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

F:\Documents and Settings\User>
```

Figure 4-2 Failed result of Ping command

Please check it following these steps:

1. Is the connection between your PC and the router correct?

Note: The 1/2/3/4 LEDs of LAN port which you link to on the router and LEDs on your PC's adapter should be lit.

2. Is the TCP/IP configuration for your PC correct?

Note: If the router's IP address is 192.168.1.1, your PC's IP address must be within the range of 192.168.1.2 ~ 192.168.1.254, the gateway must be 192.168.1.1

4.2 Quick Installation Guide

With a Web-based (Internet Explorer or Netscape® Navigator) utility, it is easy to configure and manage the NB504 54Mbps Wireless Router. The Web-based utility can be used on any Windows, Macintosh or UNIX OS with a web browser.

Connect to the router by typing `http://192.168.1.1` in the address field of web browser.



Figure 4-3 Login the router

After a moment, a login window will appear similar to that shown in Figure 4-4. Enter **admin** for the User Name and Password, both in lower case letters. Then click the **OK** button or press the **Enter** key.

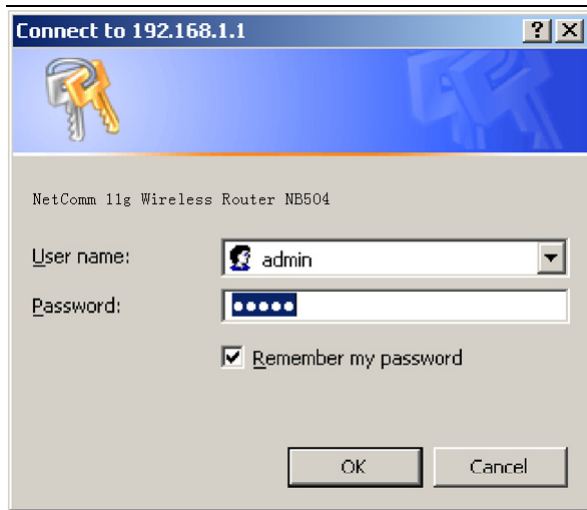
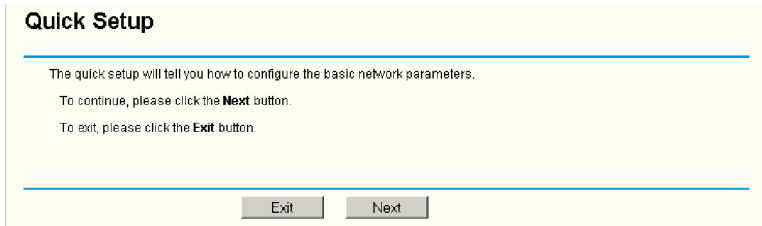


Figure 4-4 Login Windows

Note: If the above screen does not pop-up, it means that your web-browser has been set to a proxy. Go to Tools menu>Internet Options>Connections>LAN Settings, in the screen that appears, cancel the Using Proxy checkbox, and click OK to finish it.

If the User Name and Password are correct, you can configure the router using the web browser. Please click the **Quick Setup** link on the left of the main menu and the Quick Setup screen will appear.



Quick Setup

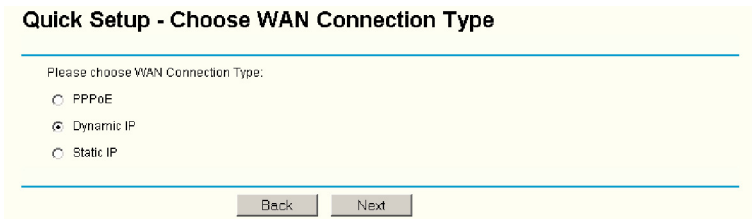
The quick setup will tell you how to configure the basic network parameters.

To continue, please click the **Next** button.

To exit, please click the **Exit** button.

Figure 4-5 Quick Setup

Click **Next**, then Choose WAN Connection Type page will appear, shown in figure 4-6.



Quick Setup - Choose WAN Connection Type

Please choose WAN Connection Type:

PPPoE

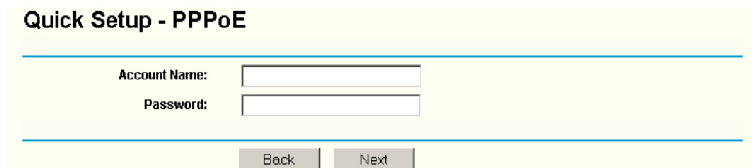
Dynamic IP

Static IP

Figure 4-6 Choose WAN Connection Type

The router supports three popular ways to connect to Internet. Please select one compatible with your ISP. Click **Next** to enter the necessary network parameters.

If you choose “PPPoE”, you will see this page shown in figure 4-7:



Quick Setup - PPPoE

Account Name:

Password:

Figure 4-7 Quick Setup - PPPoE

- **User Name and Password** - Enter the **User Name** and **Password** provided by your ISP. These fields are case sensitive. If you have difficulty with this process, please contact your ISP.

If you choose “Dynamic IP”, the router will automatically receive the IP parameters from your ISP without needing to enter any parameters.

If you Choose “Static IP”, the Static IP settings page will appear, shown in figure 4-8:

Quick Setup - Static IP

IP Address:

Subnet Mask:

Default Gateway: (Optional)

Primary DNS: (Optional)

Secondary DNS: (Optional)

Figure 4-8 Quick Setup - Static IP

Note - The IP parameters should have been provided by your ISP.

- **IP Address** - This is the WAN IP address as seen by external users on the Internet (including your ISP). Enter the IP address into the field.
- **Subnet Mask** - The Subnet Mask is used for the WAN IP address, it is usually 255.255.255.0
- **Default Gateway** - Enter the gateway IP address into the box if required.
- **Primary DNS** - Enter the DNS Server IP address into the boxes if required.
- **Secondary DNS** - If your ISP provides another DNS server, enter it into this field.

Note - For other connection types please refer to section 5.4.2

After you complete the above, click **Next**, the Wireless settings page will appear, shown in figure 4-9.

Quick Setup - Wireless

If you modify the following settings, please reboot the router manually to take effect the changes.

Wireless Radio:

SSID:

Region:

Channel:

Mode:

Figure 4-9 Quick Setup - Wireless settings

In this page, you can configure the following wireless parameters:

- **Wireless Radio** - Indicates whether the Access Point feature of the router is enabled or disabled. If disabled, the WLAN LED on the front panel will not be lit and the wireless stations will not be able to access the router. If enabled, the WLAN LED will be lit up and wireless stations will be able to access the router.
- **SSID** - Enter a value of up to 32 characters. The same SSID must be assigned to all wireless devices on your network. The default SSID is Wireless. This value is case-sensitive. For example, NETCOMM is NOT the same as Netcomm.
- **Region** - Select your region from the pull-down list. This field specifies the region where the wireless function of the router can be used. It may be illegal to use the wireless function of the router in a region other than one of those specified in this field.
- **Channel** - The current channel in use. This field determines which operating frequency will be used.
- **Mode** - Indicates the current mode **54Mbps (802.11g)**, **11Mbps (802.11b)**. If you select **54Mbps (802.11g)**, it is compatible with **11Mbps (802.11b)**.

These settings are only for basic wireless parameters, for advanced settings, please refer to Section 5.5: "Wireless."

Note: The change of wireless settings won't take effect until the router reboots! You can reboot it manually. If you need instructions as to how to do this, please refer to Section 5.11.5: "Rebooting the Router"

Click the Next button, you will then see the Finish page:

Quick Setup - Finish

Congratulations! The router is now connecting you to the Internet. For detail settings, please contact other menus if necessary.

Back

Finish

Figure 4-10 Quick Setup - Finish

After finishing all configurations of basic network parameters, please click Finish button to exit this Quick Setup.

CHAPTER 5: CONFIGURING THE ROUTER

This chapter describes each web page's key functions.

5.1 login

After your successful login, you can configure and manage the router. There are ten main menus on the left of the web-based utility. Submenus will be available after you click one of the main menus. The ten main menus are: **Status**, **Quick Setup**, **Network**, **Wireless**, **DHCP**, **Forwarding**, **Security**, **Static Routing**, **Dynamic DDNS** and **System Tools**. On the right of the web-based utility, there are the detailed explanations and instructions for the corresponding page. To apply any settings you have altered on the page, please click the Save button.

The detailed explanations for each web page key's function is listed.

5.2 Status

The Status page displays the router's current status and configuration. All information is read-only.

1. LAN

This field displays the current settings or information for the LAN, including the **MAC address**, **IP address** and **Subnet Mask**.

2. Wireless

This field displays basic information or status for wireless function, including **Wireless Radio**, **SSID**, **Channel**, **Mode**, **Wireless MAC address** and **IP address**.

3. WAN

These parameters apply to the WAN port of the router, including **MAC address**, **IP address**, **Subnet Mask**, **Default Gateway**, **DNS server** and **WAN connection type**. If PPPoE is chosen as the WAN connection type, the **Disconnect** button will be shown here while you are accessing the Internet. You can also cut the connection by clicking the button. If you have not connected to the Internet, just click **Connect** to establish the connection.

4. Traffic Statistics

This field displays the router's traffic statistics.

5. System Up Time

The amount of time from when the router was switched on or reset.

Router Status

Firmware Version: 3.5.3 Build 070511 Rel.30898n
Hardware Version: NetComm-NB504 v1.0 081520EF

LAN

MAC Address: 00-19-E0-00-00-13
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0

Wireless

Wireless Radio: Enabled
Name (SSID): Wireless
Channel: 6
Mode: 54Mbps (802.11g)
MAC Address: 00-19-E0-00-00-13
IP Address: 192.168.1.1

WAN

MAC Address: 00-19-E0-00-00-14
IP Address: 0.0.0.0 Dynamic IP
Subnet Mask: 0.0.0.0
Default Gateway: 0.0.0.0 **Obtaining Network Parameters...**
DNS Server: 0.0.0.0 , 0.0.0.0

Traffic Statistics

	Received	Sent
Bytes:	0	0
Packets:	0	0

System Up Time: 0 day(s) 00:03:58

Figure 5-1 Router Status

5.3 Quick Setup

Please refer to Section 4.2: “Quick Installation Guide.”

5.4 Network



Figure 5-2 the Network menu

There are three submenus under the Network menu (shown in figure 5-2): **LAN**, **WAN** and **MAC Clone**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

5.4.1 LAN

You can configure the IP parameters of LAN on this page.

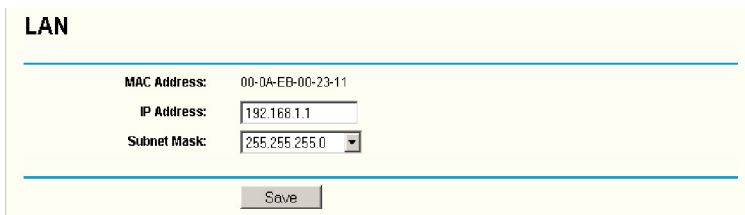
A screenshot of a web-based configuration page titled "LAN". It features three rows of configuration fields: "MAC Address" with the value "00-0A-EB-00-23-11", "IP Address" with a text input field containing "192.168.1.1", and "Subnet Mask" with a dropdown menu showing "255.255.255.0". A "Save" button is located at the bottom center of the form.

Figure 5-3 LAN

- **MAC Address** - The physical address of the router, as seen from the LAN. The value can't be changed.
- **IP Address** - Enter the IP address of your router in dotted-decimal notation (factory default: 192.168.1.1).
- **Subnet Mask** - An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.

Note:

- If you change the IP Address of LAN, you must use the new IP Address to login the router.*
- If the new LAN IP Address you set is not in the same subnet, the IP Address pool of the DHCP server will not take effect, until they are re-configured.*
- If the new LAN IP Address you set is not in the same subnet, the Virtual Server and DMZ Host will change accordingly at the same time.*

5.4.2 WAN

You can configure the WAN port parameters on this page.

First, please choose the WAN Connection Type (Dynamic IP/Static IP/PPPoE/802.1X + Dynamic IP/802.1X + Static IP/BigPond Cable/L2TP/PPTP) for Internet. The default type is **Dynamic IP**. If you aren't given any login parameters (fixed IP Address, logging ID, etc), please select **Dynamic IP**. If you are given a fixed IP (static IP), please select **Static IP**. If you are given a user name and a password, please select the type of your ISP provided (PPPoE/BigPond/L2TP/PPTP). If you are not sure which connection type you use currently, please contact your ISP to obtain the correct information.

1. If you choose **Dynamic IP**, the router will automatically get IP parameters from your ISP. You can see the page as follows (figure 5-4):

The screenshot shows the WAN configuration interface. At the top, the title is 'WAN'. Below it, the 'WAN Connection Type' is set to 'Dynamic IP'. The 'Host Name' field is empty. The 'IP Address', 'Subnet Mask', and 'Default Gateway' fields are all set to '0.0.0.0'. There are two buttons: 'Renew' and 'Release'. To the right of these buttons is the text 'Obtaining network parameters...'. Below this, the 'MTU Size (in bytes)' is set to '1500' with a note '(The default is 1500, do not change unless necessary)'. There is a checkbox 'Use These DNS Servers' which is unchecked. Below that, the 'Primary DNS' field is set to '0.0.0.0' and the 'Secondary DNS' field is set to '0.0.0.0' with '(Optional)' next to it. At the bottom, there is another checkbox 'Get IP with Unicast DHCP (It is usually not required.)' which is unchecked. A 'Save' button is at the very bottom.

Figure 5-4 WAN – Dynamic IP

This page displays the WAN IP parameters assigned dynamically by your ISP, including IP address, Subnet Mask, Default Gateway, etc. Click the **Renew** button to renew the IP parameters from your ISP. Click the **Release** button to release the IP parameters.

MTU Size - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs you need to reduce the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

If your ISP gives you one or two DNS addresses, select **Use These DNS Servers** and enter the primary and secondary addresses into the correct fields. Otherwise, the DNS servers will be assigned dynamically from your ISP.

Note: If you get an address and find error when you go to a Web site, it is likely that your DNS servers are set up improperly. You should contact your ISP to get DNS server addresses.

Get IP with Unicast DHCP - A few ISPs' DHCP servers do not support the broadcast applications. If you cannot get the IP Address normally, you can choose this option. (This is rarely required.)

2. If you choose **Static IP**, you should have fixed IP Parameters specified by your ISP. The Static IP settings page will appear, shown in figure 5-5:

WAN

WAN Connection Type:

IP Address:

Subnet Mask:

Default Gateway: (Optional)

MTU Size (in bytes): (The default is 1500, do not change unless necessary)

Primary DNS: (Optional)

Secondary DNS: (Optional)

Figure 5-5 WAN - Static IP

You should type the following parameters into the spaces provided:

- **IP Address** - Enter the IP address in dotted-decimal notation provided by your ISP.
- **Subnet Mask** - Enter the subnet Mask in dotted-decimal notation provided by your ISP, usually is 255.255.255.0.
- **Default Gateway** - (Optional) Enter the gateway IP address in dotted-decimal notation provided by your ISP.
- **MTU Size** - The normal MTU (Maximum Transmission Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs you may need to modify the MTU. But this is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.
- **Primary DNS** - (Optional) Enter the DNS address in dotted-decimal notation provided by your ISP.
- **Secondary DNS** - (Optional) Type another DNS address in dotted-decimal notation provided by your ISP if provided.

3. If you choose PPPoE, you should enter the following parameters (figure 5-6):

Figure 5-6 WAN - PPPoE

- **User Name/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Connect on Demand** - You can configure the router to disconnect your Internet connection after a specified period of inactivity (**Max Idle Time**). If your Internet connection has been terminated due to inactivity, **Connect on Demand** enables the router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, click the radio button. If you want your Internet connection to remain active at all times, enter 0 in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.

Caution: Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications are visiting the Internet continually in the background.

- **Connect Automatically** - Connect automatically after the router is disconnected. To use this option, click the radio button.
- **Time-based Connecting** - You can configure the router to make it connect or disconnect based on time. Enter the start time in HH:MM format for connecting and end time in HH:MM format for disconnecting in the Period of Time fields.

Note: Only when you have configured the system time on System Tools -> Time page, will the Time-based Connecting function can take effect.

- **Connect Manually** - You can configure the router to make it connect or disconnect manually. After a specified period of inactivity (**Max Idle Time**), the router will disconnect from the Internet connection, and you will not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. To use this option, click the radio button. If you want your Internet connection to remain active at all times, enter "0" in the **Max Idle Time** field. Otherwise, enter the number time in minutes that you wish to have the Internet connecting last unless a new link is requested.

Caution: Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications are visiting the Internet continually in the background.

Click the **Connect** button to connect immediately, Click the **Disconnect** button to disconnect immediately.

Click the **Advanced Settings** button to set up the advanced option, the page shown in figure 5-7 will then appear:

PPPoE Advanced Settings

MTU Size (in bytes): (The default is 1492, do not change unless necessary)

Service Name:

AC Name:

Use IP address specified by ISP

ISP specified IP Address:

Detect Online Interval: Seconds (0 ~ 120 seconds, 0 means not detecting.)

Use the following DNS Servers

Primary DNS:

Secondary DNS: (Optional)

Figure 5-7 PPPoE Advanced Settings

- **Packet MTU** - The default MTU size is 1492 bytes, which value is usually fine. For some ISPs, you need modify the MTU. This should not be done unless you are sure it is necessary for your ISP.
- **Service Name/AC Name** - The service name and AC (Access Concentrator) name, these should not be configured unless you are sure it is necessary for your ISP.
- **ISP Specified IP Address** - If you know that your ISP does not automatically transmit your IP address to the router during login, click “**Use the IP Address specified by ISP**” check box and enter the IP Address in dotted-decimal notation, which your ISP provided.
- **Detect Online Interval** - The default value is 0, you can input the value between 0 and 120. The router will detect Access Concentrator online at every interval between seconds. If the value is 0, it means, do not detect.
- **DNS IP address** - If you know that your ISP does not automatically transmit DNS addresses to the router during login, click “**Use the following DNS servers**” checkbox and enter the IP address in dotted-decimal notation of your ISP’s primary DNS server. If a secondary DNS server address is available, enter it as well.

Click the **Save** button to save your settings.

4. If you choose 802.1X + Dynamic IP, you should enter the follow parameters(figure 5-8) :

WAN

WAN Connection Type: 802.1X + Dynamic IP ▾

User Name:

Password:

Host Name:

IP Address: 0.0.0.0

Subnet Mask: 0.0.0.0

Default Gateway: 0.0.0.0

MTU Size (in bytes): 1500 (The default is 1500, do not change unless necessary.)

Use These DNS Servers

Primary DNS: 0.0.0.0

Secondary DNS: 0.0.0.0 (Optional)

Get IP with Unicast DHCP (It is usually not required.)

Figure 5-8 802.1X + Dynamic IP Settings

- **User Name** - Enter the user name for 802.1X authentication provided by your ISP
- **Password** - Enter the password for 802.1X authentication provided by your ISP.
[Click Login](#) to start 802.1X authentication.
[Click Logout](#) to end 802.1X authentication.
- **Host Name** - This field is required to be filled by some service provider.

5. If you choose 802.1X + Static IP, you should enter the follow parameters (figure 5-9) :

WAN

WAN Connection Type:

User Name:

Password:

IP Address:

Subnet Mask:

Default Gateway: (Optional)

MTU Size (in bytes): (The default is 1500, do not change unless necessary)

Primary DNS: (Optional)

Secondary DNS: (Optional)

Figure 5-9 802.1X + Static IP Settings

- **User Name** - Enter the user name for 802.1X authentication provided by your ISP
- **Password** - Enter the password for 802.1X authentication provided by your ISP.
[Click Login](#) to start 802.1X authentication.
[Click Logout](#) to end 802.1X authentication.
- **IP Address** - Enter the IP address in dotted-decimal notation provided by your ISP.
- **Subnet Mask** - Enter the subnet Mask in dotted-decimal notation provided by your ISP.
- **Default Gateway** - (Optional) Enter the default gateway IP address in dotted-decimal notation provided by your ISP.

6. If you choose **BigPond Cable**, you should enter the following parameters (figure 5-10):

WAN

WAN Connection Type:

User Name:

Password:

Auth Server:

Auth Domain:

MTU Size (in bytes): (The default is 1500, do not change unless necessary.)

Connect on Demand
 Max Idle Time: minutes (0 means remain active at all times.)

Connect Automatically

Connect Manually
 Max Idle Time: minutes (0 means remain active at all times.)

Disconnected

Figure 5-10 BigPond Settings

- **User Name/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Auth Server** - Enter the authenticating server IP address or host name.
- **Auth Domain** - Type in the domain suffix server name based on your location. Eg,
 NSW / ACT - nsw.bigpond.net.au
 VIC / TAS / WA / SA / NT - vic.bigpond.net.au
 QLD - qld.bigpond.net.au
- **Connect on Demand** - You can configure the router to disconnect from your Internet connection after a specified period of inactivity (**Max Idle Time**). If your Internet connection has been terminated due to inactivity, **Connect on Demand** enables the router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, click the radio button. If you want your Internet connection to remain active at all times, enter 0 in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.

Caution: Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications are visiting the Internet continually in the background.

- **Connect Automatically** - Connect automatically after the router is disconnected. To use this option, click the radio button.
- **Connect Manually** - You can configure the router to make it connect or disconnect manually. After a specified period of inactivity (**Max Idle Time**), the router will disconnect from your Internet connection, and you will not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. To use this option, click the radio button. If you want your Internet connection to remain active at all times, enter "0" in the **Max Idle Time** field. Otherwise, enter the number in minutes that you wish to have the Internet connecting last unless a new link is requested.

Caution: Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications are visiting the Internet continually in the background.

- Click the **Connect** button to connect immediately, Click the **Disconnect** button to disconnect immediately.

7. If you choose L2TP, you should enter the following parameters (figure 5-11):

WAN

WAN Connection Type:

User Name:

Password:

Disconnected!

Dynamic IP Static IP

Server IP Address/Name:

IP Address:

Subnet Mask:

Gateway:

DNS:

Internet IP Address: 0.0.0.0

Internet DNS: 0.0.0.0, 0.0.0.0

MTU Size (in bytes): (The default is 1460, do not change unless necessary.)

Max Idle Time: minutes (0 means remain active at all times.)

WAN Connection Mode: Connect on Demand
 Connect Automatically
 Connect Manually

Figure 5-11 L2TP Settings

- **User Name/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Dynamic IP/ Static IP** – Choose either as you are given by your ISP.
Click the **Connect** button to connect immediately, Click the **Disconnect** button to disconnect immediately.
- **Connect on Demand** - You can configure the router to disconnect from your Internet connection after a specified period of inactivity (**Max Idle Time**). If your Internet connection has been terminated due to inactivity, **Connect on Demand** enables the router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, click the radio button. If you want your Internet connection to remain active at all times, enter 0 in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.

Caution: Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications is visiting the Internet continually in the background.

- **Connect Automatically** - Connect automatically after the router is disconnected. To use this option, click the radio button.
- **Connect Manually** - You can configure the router to make it connect or disconnect manually. After a specified period of inactivity (**Max Idle Time**), the router will disconnect from your Internet connection, and you will not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. To use this option, click the radio button. If you want your Internet connection to remain active at all times, enter "0" in the **Max Idle Time** field. Otherwise, enter the number in minutes that you wish to have the Internet connecting last unless a new link is requested.

Caution: Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications are visiting the Internet continually in the background.

8. If you choose PPTP, you should enter the following parameters (figure 5-12):

WAN

WAN Connection Type:

User Name:

Password:

Disconnected!

Dynamic IP Static IP

Server IP Address/Name:

IP Address:

Subnet Mask:

Gateway:

DNS:

Internet IP Address: 0.0.0.0

Internet DNS: 0.0.0.0, 0.0.0.0

MTU Size (in bytes): (The default is 1420, do not change unless necessary.)

Max Idle Time: minutes (0 means remain active at all times.)

Wan Connection Mode:

Connect on Demand
 Connect Automatically
 Connect Manually

Figure 5-12 PPTP Settings

- **User Name/Password** - Enter the User Name and Password provided by your ISP. These fields are case-sensitive.
- **Dynamic IP/ Static IP** – Choose either as you are given by your ISP and enter the ISP's IP address or the domain name.

If you choose static IP and enter the domain name, you should also enter the DNS assigned by your ISP. And click the **Save** button.

Click the **Connect** button to connect immediately, Click the **Disconnect** button to disconnect immediately.

- **Connect on Demand** - You can configure the router to disconnect from your Internet connection after a specified period of inactivity (**Max Idle Time**). If your Internet connection has been terminated due to inactivity, **Connect on Demand** enables the router to automatically re-establish your connection as soon as you attempt to access the Internet again. If you wish to activate **Connect on Demand**, click the radio button. If you want your Internet connection to remain active at all times, enter "0" in the **Max Idle Time** field. Otherwise, enter the number of minutes you want to have elapsed before your Internet connection terminates.

Caution: Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications are visiting the Internet continually in the background.

- **Connect Automatically** - Connect automatically after the router is disconnected. To use this option, click the radio button.
- **Connect Manually** - You can configure the router to make it connect or disconnect manually. After a specified period of inactivity (**Max Idle Time**), the router will disconnect from your Internet connection, and you will not be able to re-establish your connection automatically as soon as you attempt to access the Internet again. To use this option, click the radio button. If you want your Internet connection to remain active at all times, enter "0" in the **Max Idle Time** field. Otherwise, enter the number in minutes that you wish to have the Internet connecting last unless a new link is requested.

Caution: Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications are visiting the Internet continually in the background.

5.4.3 MAC Clone

You can configure the MAC address of the WAN port on this page, figure 5-13:

MAC Clone

WAN MAC Address:	<input type="text" value="00-0A-EB-00-23-12"/>	<input type="button" value="Restore Factory MAC"/>
Your PC's MAC Address:	<input type="text" value="00-13-8F-AA-6D-77"/>	<input type="button" value="Clone MAC Address"/>

Figure 5-13 MAC Address Clone

Some ISPs require that you register the MAC Address of your adapter, which is connected to your cable, DSL modem or Ethernet during installation. Changes are rarely needed here.

- **WAN MAC Address** - This field displays the current MAC address of the WAN port, which is used for the WAN port. If your ISP requires that you register the MAC address, please enter the correct MAC address into this field. The format for the MAC Address is XX-XX-XX-XX-XX-XX (X is any hexadecimal digit).
- **Your PC's MAC Address** - This field displays the MAC address of the PC that is managing the router. If the MAC address is required, you can click the **Clone MAC Address** button and this MAC address will fill in the **WAN MAC Address** field.

Click **Restore Factory MAC** to restore the MAC address of WAN port to the factory default value.

Click the **Save** button to save your settings.

Note:

- 1) *Only the PC on your LAN can use the MAC Address Clone feature.*
- 2) *If you click the Save button, the router will prompt you to reboot.*

5.5 Wireless

- **Wireless**
 - **Wireless Settings**
 - **MAC Filtering**
 - **Wireless Statistics**

Figure 5-14 Wireless menu

There are three submenus under the Wireless menu (shown in figure 5-14): **Wireless Settings**, **MAC Filtering** and **Wireless Statistics**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

5.5.1 Wireless Settings

The basic settings for the wireless network are set on this page, figure 5-15:

Wireless Settings

SSID:

Region:

Channel:

Mode:

Enable Wireless Router Radio

Enable SSID Broadcast

Enable Wireless Security

Security Type:

Security Option:

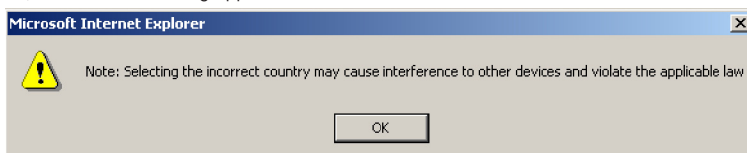
WEP Key Format:

Key Selected	WEP Key	Key Type
Key 1: <input type="radio"/>	<input type="text"/>	<input type="text" value="Disabled"/>
Key 2: <input type="radio"/>	<input type="text"/>	<input type="text" value="Disabled"/>
Key 3: <input type="radio"/>	<input type="text"/>	<input type="text" value="Disabled"/>
Key 4: <input type="radio"/>	<input type="text"/>	<input type="text" value="Disabled"/>

Figure 5-15 Wireless Settings

- **SSID** - Enter a value of up to 32 characters. The same name (SSID) must be assigned to all wireless devices in your network. The default SSID is Wireless, but it is recommended strongly that you change your networks name (SSID) to a different value. This value is case-sensitive. For example, NETCOMM is NOT the same as Netcomm.
- **Region** - Select your region from the pull-down list. This field specifies the region where the wireless function of the router can be used. It may be illegal to use the wireless function of the router in a region other than one of those specified in this field. If your country or region is not listed, please contact your local government agency for assistance.

The default region is Australia. When you select your local region from the pull-down list, Click the **Save** button, then the Note Dialog appears. Click OK.



Note Dialog

- **Channel** - This field determines which operating frequency will be used. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- **Mode** - Select the desired wireless mode. The options are:
 - **54Mbps (802.11g)** - Both 802.11g and 802.11b wireless stations can connect to the router.
 - **11Mbps (802.11b)** - Only 802.11b wireless stations can connect to the router.

Note: The default is "54Mbps (802.11g)", which allows both 802.11g and 802.11b wireless stations to connect to the router.
- **Enable Wireless Router Radio** - The wireless radio of this Router can be enabled or disabled to allow wireless stations access. If enabled, wireless stations will be able to access the router, otherwise, wireless stations will not be able to access.
- **Enable SSID Broadcast** - If you select the **Enable SSID Broadcast** checkbox, the Wireless Router SSID will broadcast its name (SSID) on the air.
- **Enable Wireless Security** – The wireless security function can be enabled or disabled. If disabled, the wireless stations will be able to connect the router without encryption. It is recommended strongly that you choose this option to encrypt your wireless network. The encryption settings described below.
- **Security Type** - You can select one of the following Security types:
 - **WEP** - Select WEP authentication type based on 802.11 authentications.
 - **WPA-PSK/WPA2-PSK** - Select WPA/WPA2 authentication type based on pre-shared passphrase.
 - **WPA /WPA2** - Select WPA/WPA2 authentication type based on Radius Server.
- **Security Options** - You can select one of the following authentication options:
 - When you select **WEP** for Security type you can select the following Security options:
 - **Automatic** - Select Shared Key or Open System authentication type automatically based on the wireless station request.
 - **Shared Key** - Select 802.11 Shared Key authentication.
 - **Open System** - Select 802.11 Open System authentication.
 - When you select **WPA-PSK/WPA2-PSK** for Security type you can select **Automatic, WPA –PSK or WPA2-PSK** as Security options.
 - When you select **WPA/WPA2** as an Security type you can select **Automatic WPA or WPA2** as Security option.
- **WEP Key Format** - You can select **ASCII** or **Hexadecimal** format. ASCII Code Format stands for any combination of keyboard characters in the specified length. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length.
- **WEP Key settings** - Select which of the four keys will be used and enter the matching WEP key information for your network in the selected key radio button. These values must be identical on all wireless stations in your network.
- **Key Type** - You can select the WEP key length (**64-bit**, or **128-bit**, or **152-bit**) for encryption. "Disabled" means the WEP key entry is invalid.
 - **For 64-bit encryption** - You can enter 10 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 5 ASCII characters.
 - **For 128-bit encryption** - You can enter 26 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 13 ASCII characters.
 - **For 152-bit encryption** - You can enter 32 hexadecimal digits (any combination of 0-9, a-f, A-F, zero key is not permitted) or 16 ASCII characters.
- **Encryption** - When you select **WPA-PSK/WPA2-PSK** or **WPA/WPA2** for Authentication Type you can select either **Automatic, TKIP** or **AES** as Encryptions.

Security Type:	<input type="text" value="WPA-PSK/WPA2-PSK"/>
Security Option:	<input type="text" value="Automatic"/>
Encryption:	<input type="text" value="Automatic"/>
PSK Passphrase:	<input type="text"/>
	(The Passphrase is between 8 and 63 characters long)
Group Key Update Period:	<input type="text" value="30"/> (in second, minimum is 30, 0 means no update)

Figure 5-15a WPA-PSK/WPA2-PSK

- **WPA-PSK/WPA2-PSK Passphrase** - You can enter a WPA or WPA2 passphrase between 8 and 63 characters long.
- **Group Key Update Period** - Specify the group key update interval in seconds. The value can be either 0 seconds or from 30 seconds and up, 1-29 seconds are not usable figures. Enter 0 to disable the update.

Security Type:	<input type="text" value="WPA/WPA2"/>
Security Option:	<input type="text" value="Automatic"/>
Encryption:	<input type="text" value="Automatic"/>
Radius Server IP:	<input type="text"/>
Radius Port:	<input type="text" value="1812"/> (1-65535, 0 means the default port 1812)
Radius password:	<input type="text"/>
Group Key Update Period:	<input type="text" value="30"/> (in second, minimum is 30, 0 means no update)

Figure 5-15b WPA/WPA2

- **Radius Server IP** - Enter the IP address of the Radius Server
- **Radius Port** - Enter the port number that the radius service used.
- **Radius Password** - Enter the password for the Radius Server.

Be sure to click the **Save** button to save your settings on this page.

Note: The router will reboot automatically after you click save.

5.5.2 MAC Filtering

The Wireless MAC Filtering for wireless networks are set on this page, figure 5-16:

Figure 5-16 Wireless MAC address Filtering

The Wireless MAC Address Filtering feature allows you to control wireless stations accessing the router, which depend on the station's MAC addresses.

- **MAC Address** - The wireless station's MAC address that you want to access.
- **Status** - The status of this entry either **Enabled** or **Disabled**.
- **Privilege** - Select the privileges for this entry. You may select one of the following **Allow / Deny / 64-bit / 128-bit / 152-bit**.
- **Description** - A simple description of the wireless station.
- **WEP Key** - Specify a unique WEP key (in Hexadecimal format) to access the router.

To set up an entry, follow these instructions:

First, you must decide whether the unspecified wireless stations can access the router or not. If you desire that the unspecified wireless stations can access the router, please select the radio button **Allow the stations not specified by any enabled entries in the list to access**, otherwise, select the radio button **Deny the stations not specified by any enabled entries in the list to access**.

To Add a Wireless MAC Address filtering entry, click the **Add New...** button. The "Add or Modify Wireless MAC Address Filtering entry" page will appear, shown in figure 5-17:

Figure 5-17 Add or Modify Wireless MAC Address Filtering entry

To add or modify a MAC Address Filtering entry, follow these instructions:

1. Enter the appropriate MAC Address into the **MAC Address** field. The format of the MAC Address is XX-XX-XX-XX-XX (X is any hexadecimal digit). For example: 00-0A-EB-B0-00-0B.
2. Enter a simple description of the wireless station in the **Description** field. For example: Wireless station A.
3. **Privilege** - Select the privileges for this entry, one of **Allow / Deny / 64-bit / 128-bit / 152-bit**.
4. **WEP Key** - If you select **64-bit, 128-bit** or **152-bit** in the **Privilege** field, enter any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length. For example: 2F34D20BE2.
5. **Status** - Select **Enabled** or **Disabled** for this entry on the Status pull-down list.
6. Click the **Save** button to save this entry.

To add additional entries, repeat steps 1-6.

Note: When 64-bit, or 128-bit, or 152-bit is selected, WEP Key will be enabled.

To modify or delete an existing entry:

1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable All** button to make all entries enabled

Click the **Disabled All** button to make all entries disabled.

Click the **Delete All** button to delete all entries

Click the **Next** button to go to the next page and click the Previous button to return to the previous page.

For example: If you desire that the wireless station A with MAC address 00-0A-EB-00-07-BE be able to access the router. The wireless station B with MAC address 00-0A-EB-00-07-5F not be able to access the router, and the wireless station C with MAC address 00-0A-EB-00-07-8A be able to access the router when its WEP key is 2F34D20BE2E 54B326C5476586A, while all other wireless stations cannot access the router, you should configure the **Wireless MAC Address Filtering** list by following these steps:

1. Click the **Enable** button to enable this function.
2. Select the radio button: **Deny the stations not specified by any enabled entries in the list to access for Filtering Rules**.
3. Delete all or disable all entries if there are any entries already.
4. Click the **Add New...** button and enter the MAC address 00-0A-EB-00-07-BE in the **MAC Address** field, enter wireless station A in the **Description** field, select **Allow** in the **Privilege** pull-down list and select **Enabled** in the Status pull-down list. Click the **Save** and the **Return** button.
5. Click the **Add New...** button and enter the MAC address 00-0A-EB-00-07-5F in the **MAC Address** field, enter wireless station B in the **Description** field, select **Deny** in the **Privilege** pull-down list and select **Enabled** in the Status pull-down list. Click the **Save** and the **Return** button.
6. Click the **Add New...** button and enter the MAC address 00-0A-EB-00-07-8A in the **MAC Address** field, enter wireless station C in the **Description** field, select **128-bit** in the **Privilege** pull-down list, enter 2F34D20BE2E54B326C5476586A in the **WEP Key** field and select **Enabled** in the Status pull-down list. Click the **Save** and the **Return** button.

The filtering rules that configured should be similar to the following list:

ID	MAC Address	Status	Privilege	<input checked="" type="radio"/> Description <input type="radio"/> WEP Key	Modify
1	00-0A-EB-00-07-8E	Enabled	allow	Wireless Station A	Modify Delete
2	00-0A-EB-00-07-5F	Enabled	deny	Wireless Station B	Modify Delete
3	00-0A-EB-00-07-8A	Enabled	128 bit	Wireless Station C	Modify Delete

Note:

- a) *If you select the radio button Allow the stations not specified by any enabled entries in the list to access for Filtering Rules, the wireless station B will still not be able to access the router, however, other wireless stations that are not in the list will be able to access the router.*
- b) *If you enable the function and select the Deny the stations not specified by any enabled entries in the list to access for Filtering Rules, and there are not any enable entries in the list, thus, no wireless stations can access the router.*

5.5.3 Wireless Statistics

This page shows **MAC Address**, **Current Status**, **Received Packets** and **Sent Packets** for each connected wireless station.

Wireless Statistics

Current Connected Wireless Stations numbers: **1**

ID	MAC Address	Current Status	Received Packets	Sent Packets
1	00-0A-EB-00-23-11	AP-UP	0	941

Figure 5-18 The router attached wireless stations

- **MAC Address** - The connected wireless station's MAC address
- **Current Status** - The connected wireless station's running status, one of STA-AUTH / STA-ASSOC / AP-UP / WPA / WPA-PSK /WPA2/WPA2-PSK/None
- **Received Packets** - Packets received by the station
- **Sent Packets** - Packets sent by the station

You cannot change any of the values on this page. To update this page and to show the current connected wireless stations, click on the **Refresh** button.

If the numbers of connected wireless stations go beyond one page, click the **Next** button to go to the next page and click the **Previous** button to return the previous page.

Note: This page will be refreshed automatically every 5 seconds.

5.6 DHCP

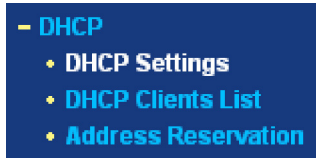


Figure 5-19 The DHCP menu

There are three submenus under the DHCP menu (shown in figure 5-19): **DHCP Settings**, **DHCP Clients List** and **Address Reservation**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

5.6.1 DHCP Settings

The router is set up by default as a DHCP (Dynamic Host Configuration Protocol) server, which provides the TCP/IP configuration for all the PCs that are connected to the router on the LAN. The DHCP Server can be configured on the page (shown in figure 5-20):

DHCP Settings

DHCP Server: Disable Enable

Start IP Address:

End IP Address:

Address Lease Time: minutes (1 ~ 2880 minutes, the default value is 120)

Default Gateway: (optional)

Default Domain: (optional)

Primary DNS: (optional)

Secondary DNS: (optional)

Figure 5-20 DHCP Settings

- **DHCP Server - Enable or Disable** the DHCP server. If you disable the Server, you must have another DHCP server within your network or else you must manually configure the computer.
- **Start IP Address** - This field specifies the first of the addresses in the IP address pool. 192.168.1.100 is the default start address.
- **End IP Address** - This field specifies the last of the addresses in the IP address pool. 192.168.1.199 is the default end address.
- **Address Lease Time** - The **Address Lease Time** is the amount of time in which a network user will be allowed connection to the router with their current dynamic IP Address. Enter the amount of time, in minutes. The user will be “leased” this dynamic IP Address. The range of the time is 1 ~ 2880 minutes. The default value is 120 minutes.
- **Default Gateway** - (Optional.) Suggest to input the IP address of the LAN port of the router, default value is 192.168.1.1
- **Default Domain** - (Optional.) Input the domain name of your network.
- **Primary DNS** - (Optional.) Input the DNS IP address provided by your ISP. Or consult your ISP.
- **Secondary DNS** - (Optional.) Input the IP address of another DNS server if your ISP provides two DNS servers.

Note: To use the DHCP server function of the router, you must configure all computers on the LAN as “Obtain an IP Address automatically” mode. This function will take effect until the router reboots.

5.6.2 DHCP Clients List

This page shows **Client Name**, **MAC Address**, **Assigned IP** and **Lease Time** for each DHCP Client attached to the router (figure 5-21):

DHCP Clients List				
ID	Client Name	MAC Address	Assigned IP	Lease Time
1	Anthea	00-13-BF-AA-6D-77	192.168.1.100	01:59:29

Figure 5-21 DHCP Clients List

- **Index** - The index of the DHCP Client
- **Client Name** - The name of the DHCP client
- **MAC Address** - The MAC address of the DHCP client
- **Assigned IP** - The IP address that the router has allocated to the DHCP client.
- **Lease Time** - The time of the DHCP client leased. Before the time is up, DHCP client will request to renew the lease automatically.

You cannot change any of the values on this page. To update this page and to show the current attached devices, click on the **Refresh** button.

5.6.3 Address Reservation

When you specify a reserved IP address for a PC on the LAN, that PC will always receive the same IP address each time when it accesses the DHCP server. Reserved IP addresses should be assigned to servers that require permanent IP settings. This page is used for address reservation (shown in figure 5-22).

Address Reservation				
ID	MAC Address	Reserved IP Address	Status	Modify
1	00-04-EB-00-23-11	192.168.1.100	Enabled	Modify Delete

Figure 5-22 Address Reservation

- **MAC Address** - The MAC address of the PC of which you want to reserve IP address.
- **Assigned IP Address** - The IP address of the router reserved.
- **Status** - The status of this entry either Enabled or Disabled.

To Reserve IP addresses:

1. Click the **Add New** button. (Pop-up figure 5-23)
2. Enter the MAC address (The format for the MAC Address is XX-XX-XX-XX-XX-XX.) and IP address in dotted-decimal notation of the computer you wish to add.
3. Click the **Save** button when finished.

Add or Modify a Address Reservation Entry

MAC Address:	<input type="text"/>
Reserved IP Address:	<input type="text"/>
Status:	<input type="text" value="Enabled"/>

Figure 5-23 Add or Modify a Address Reservation Entry

To modify or delete an existing entry:

1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable All** button to make all entries enabled

Click the **Disabled All** button to make all entries disabled.

Click the **Delete All** button to delete all entries

Click the **Next** button to go to the next page and Click the **Previous** button to return the previous page.

Note: The function won't take effect until the router reboots.

5.7 Forwarding

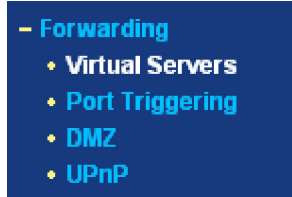


Figure 5-24 The Forwarding menu

There are four submenus under the Forwarding menu (shown in figure 5-24): **Virtual Servers**, **Port Triggering**, **DMZ** and **UPnP**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

5.7.1 Virtual Servers

Virtual servers can be used for setting up public services on your LAN, such as DNS, Email and FTP. A virtual server is defined as a service port, and all requests from the Internet to this service port will be redirected to the computer specified by the server IP.

Any PC that was used for a virtual server must have a static or reserved IP Address because its IP Address may change when using the DHCP function. You can set up virtual servers on this page, shown in figure 5-25:

Virtual Servers

ID	Service Port	IP Address	Protocol	Status	Modify
1	21	192.168.1.101	ALL	Enabled	Modify Delete

Figure 5-25 Virtual Servers

- **Service Port** - The numbers of External Ports. You can type a service port or a range of service ports (the format is XXX – YYY, XXX is Start port, YYY is End port).
- **IP Address** - The IP Address of the PC providing the service application.
- **Protocol** - The protocol used for this application, either **TCP**, **UDP**, or **All** (all protocols supported by the router).
- **Status** - The status of this entry either **Enabled** or **Disabled**.

To setup a virtual server entry:

1. Click the **Add New** button. (pop-up figure 5-26)
2. Select the service you want to use from the **Common Service Port** list. If the Common Service Port list does not have the service that you want to use, type the number of the service port or service port range in the **Service Port** box.
3. Type the IP Address of the computer in the **Server IP Address** box.
4. Select the protocol used for this application, either **TCP** or **UDP**, or **All**.
5. Select the **Enable** checkbox to enable the virtual server.
6. Click the **Save** button.

Add or Modify a Virtual Server Entry

Service Port:

IP Address:

Protocol:

Status:

Common Service Port:

Figure 5-26 Add or Modify a Virtual Server Entry

Note: It is possible that you have a computer or server that has more than one type of available service. If so, select another service, and enter the same IP Address for that computer or server.

To modify or delete an existing entry:

1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable All** button to make all entries enabled

Click the **Disabled All** button to make all entries disabled.

Click the **Delete All** button to delete all entries

Click the **Next** button to go to the next page and Click the **Previous** button to return the previous page.

Note: If you set the virtual server of service port as 80, you must set the web management port on Security → Remote Management page to be any value except 80 such as 8080. Or else there will be a conflict to disable the virtual server.

5.7.2 Port Triggering

Some applications require multiple connections, like Internet games, video conferencing, Internet calling and so on. These applications cannot work with a pure NAT router. Port Triggering is used for some of these applications that can work with an NAT router. You can set up Port Triggering on this page shown in figure 5-27:

Port Triggering						
ID	Trigger Port	Trigger Protocol	Incoming Ports	Incoming Protocol	Status	Modify
1	554	ALL	6970-8999	ALL	Enabled	Modify Delete

Figure 5-27 Port Triggering

Once configured, operation is as follows:

1. A local host makes an outgoing connection using a destination port number defined in the Trigger Port field.
 2. The router records this connection, opens the incoming port or ports associated with this entry in the Port Triggering table, and associates them with the local host.
 3. When necessary the external host will be able to connect to the local host using one of the ports defined in the Incoming Ports field.
- **Trigger Port** - The port for outgoing traffic. An outgoing connection using this port will "Trigger" this rule.
 - **Trigger Protocol** - The protocol used for Trigger Ports, either **TCP**, **UDP**, or **All** (all protocols supported by the router).
 - **Incoming Ports Range** - The port or port range used by the remote system when it responds to the outgoing request. A response using one of these ports will be forwarded to the PC that triggered this rule. You can input at most 5 groups of ports (or port section). Every group of ports must be set apart with ",". For example, 2000-2038, 2050-2051, 2085, 3010-3030.
 - **Incoming Protocol** - The protocol used for Incoming Ports Range, either **TCP** or **UDP**, or **ALL** (all protocols supported by the router).
 - **Status** - The status of this entry either **Enabled** or **Disabled**.

To add a new rule, enter the following data on the **Port Triggering** screen.

1. Click the **Add New** button. (pop-up figure 5-28)
2. Enter a port number used by the application when it generates an outgoing request.
3. Select the protocol used for **Trigger Port** from the pull-down list, either **TCP**, **UDP**, or **All**.
4. Enter the range of port numbers used by the remote system when it responds to the PC's request.
5. Select the protocol used for **Incoming Ports Range** from the pull-down list, either **TCP** or **UDP**, or **All**.
6. Select the **Enable** checkbox to enable.
7. Click the **Save** button to save the new rule.

Add or Modify a Port Triggering Entry

Trigger Port:

Trigger Protocol: ALL

Incoming Ports:

Incoming Protocol: ALL

Status: Enabled

Common Applications: -Select One-

Save Return

Figure 5-28 Add or Modify a Triggering Entry

There are many popular applications in the **Common Applications** list. You can select it, and the application will fill in the **Trigger Port**, **incoming Ports Range** boxes and select the **Enable** checkbox. It has the same effect as adding a new rule.

To modify or delete an existing entry:

1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable All** button to make all entries enabled

Click the **Disabled All** button to make all entries disabled.

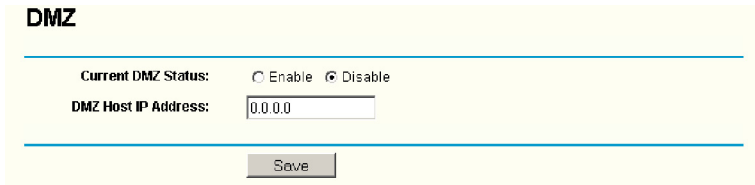
Click the **Delete All** button to delete all entries

Note:

1. *When the trigger connection is released, the according opening ports will be closed.*
2. *Each rule allowed to be used only by one host on LAN synchronously. The trigger connection of other hosts on LAN will be refused.*
3. *Incoming Port Range cannot overlap each other.*

5.7.3 DMZ

The DMZ host feature allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing. DMZ host forwards all the ports at the same time. Any PC whose port is being forwarded must have its DHCP client function disabled and should have a new static IP Address assigned to it because its IP Address may change when using the DHCP function. You can set up DMZ host on this page shown in figure 5-29:



DMZ

Current DMZ Status: Enable Disable

DMZ Host IP Address:

Save

Figure 5-29 DMZ

To assign a computer or server to be a DMZ server:

1. Click the **Enable** radio button
2. Enter the local host IP Address in the **DMZ Host IP Address** field
3. Click the **Save** button.

Note: After you set the DMZ host, the firewall related to the host will not work.

5.7.4 UPnP

The Universal Plug and Play (UPnP) feature allows the devices, such as Internet computers, to access the local host resources or devices as needed. UPnP devices can be automatically discovered by the UPnP service application on the LAN. You can configure UPnP on this page that shown in figure 5-30:

UPnP

Current UPnP Status: **Disabled**

Current UPnP Settings List

ID	App Description	External Port	Protocol	Internal Port	IP Address	Status
----	-----------------	---------------	----------	---------------	------------	--------

Figure 5-30 UPnP Settings

- **Current UPnP Status** - UPnP can be enabled or disabled by clicking the **Enable** or **Disable** button. As allowing this may present a risk to security, this feature is disabled by default.
- **Current UPnP Settings List** - This table displays the current UPnP information.
 - **App Description** – The description provided by the application in the UPnP request
 - **External Port** - External port, which the router opened for the application.
 - **Protocol** - Which type of protocol is opened.
 - **Internal Port** - Internal port, which the router opened for local host.
 - **IP Address** - The UPnP device that is currently accessing the router.
 - **Status** - Either **Enabled** or **Disabled**, “Enabled” means that port is still active, otherwise, the port is inactive.

Click Refresh to update the Current UPnP Settings List.

5.8 Security



Figure 5-31 The Security menu

There are six submenus under the Security menu (shown in figure 5-31): **Firewall**, **IP Address Filtering**, **Domain Filtering**, **MAC Filtering**, **Remote Management** and **Advanced Security**. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

5.8.1 Firewall

Using the Firewall page (shown in figure 5-32), you can turn the general firewall switch on or off. The default setting for the switch is off. If the general firewall switch is off, even if IP Address Filtering, DNS Filtering and MAC Filtering are enabled, their settings are ineffective.

Firewall

Enable Firewall (the general firewall switch)

Enable IP Address Filtering

Default IP Address Filtering Rules:

Allow the packets not specified by any filtering rules to pass through the router

Deny the packets not specified by any filtering rules to pass through the router

Enable Domain Filtering

Enable MAC Address Filtering

Default MAC Address Filtering Rules:

Allow these PCs with enabled rules to access the Internet

Deny these PCs with enabled rules to access the Internet

Save

Figure 5-32 Firewall Settings

- **Enable Firewall** - the general firewall switch is on or off.
- **Enable IP Address Filtering** - set IP Address Filtering is enabled or disabled.
There are two default filtering rules of IP Address Filtering, either Allow or Deny passing through the router.
- **Enable Domain Filtering** - set Domain Filtering is enabled or disabled.
- **Enable MAC Filtering** - set MAC Address Filtering is enabled or disabled. You can select the default filtering rules of MAC Address Filtering, either Allow or Deny accessing the router.

5.8.2 IP Address Filtering

The IP address Filtering feature allows you to control Internet Access by specific users on your LAN based on their IP addresses. The IP address filtering are set on this page, figure 5-33:

Figure 5-33 IP address Filtering

To disable the IP Address Filtering feature, keep the default setting, **Disabled**. To set up an IP Address Filtering entry, click **Enable Firewall** and **Enable IP Address Filtering** on the Firewall page, and click the **Add New...** button. The page “Add or Modify an IP Address Filtering entry” will appear shown in figure 5-34:

Figure 5-34 Add or Modify an IP Address Filtering Entry

To create or modify an IP Address Filtering entry, please follow these instructions:

1. **Effective Time** - Enter a range of time in HHMM format, which point to the range time for the entry to take effect. For example, 0803 - 1705, the entry will take effect from 08:03 to 17:05.
2. **LAN IP Address** - Enter a LAN IP Address or a range of LAN IP addresses in the field, in dotted-decimal notation format. For example, 192.168.1.20 - 192.168.1.30. Keep the field open, which means all LAN IP Addresses have been put into the field.
3. **LAN Port** - Enter a LAN Port or a range of LAN ports in the field. For example, 1030 - 2000. Keep the field open, which means all LAN ports have been put into the field.
4. **WAN IP Address** - Enter a WAN IP Address or a range of WAN IP Addresses in the field, in dotted-decimal notation format. For example, 61.145.238.6 – 61.145.238.47. Keep the field open, which means all WAN IP Addresses have been put into the field.
5. **WAN Port** - Enter a WAN Port or a range of WAN Ports in the field. For example, 25 – 110. Keep the field open, which means all WAN Ports have been put into the field.
6. **Protocol** - Select which protocol is to be used, either TCP, UDP, or All (all protocols supported by the router).

7. **Pass** - Select either **Allow** or **Deny** through the router.
8. **Status** - Select **Enabled** or **Disabled** for this entry on the **Status** pull-down list.
9. Click the **Save** button to save this entry.

To modify or delete an existing entry:

1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable All** button to make all entries enabled

Click the **Disabled All** button to make all entries disabled.

Click the **Delete All** button to delete all entries

You can change the entry's order as desired. Fore entries are before hind entries. Enter the ID number in the first box you want to move and another ID number in second box you want to move to, and then click the **Move** button to change the entry's order.

Click the **Next** button to the next page and click the **Previous** button to return to the previous page.

For example: If you desire to block E-mail received and sent by the IP Address 192.168.1.7 on your local network, and to make the PC with IP Address 192.168.1.8 unable to visit the website of IP Address 202.96.134.12, while other PCs have no limit you should specify the following IP address filtering list:

ID	Effective time	LAN IP	LAN Port	WAN IP	WAN Port	Protocol	Action	Status	Modify
1	0000-2400	192.168.1.7	-	-	25	ALL	Deny	Enabled	Modify Delete
2	0000-2400	192.168.1.7	-	-	110	ALL	Deny	Enabled	Modify Delete
3	0000-2400	192.168.1.8	-	202.96.134.12	-	ALL	Deny	Enabled	Modify Delete

5.8.3 Domain Filtering

The Domain Filtering page (shown in figure 5-35) allows you to control access to certain websites on the Internet by specifying their domains or key words.

Domain Filtering

Firewall Settings (You can change it on Firewall page)

Enable Firewall: Enabled

Enable Domain Filtering: Disabled

ID	Effective time	Domain Name	Status	Modify
<div style="display: flex; justify-content: space-between; align-items: center;"> Add New... Enable All Disable All Delete All </div>				

Previous Next

Figure 5-35 Domain Filtering

Before adding a Domain Filtering entry, you must ensure that Enable Firewall and Enable Domain Filtering have been selected on the Firewall page. To Add a Domain filtering entry, click the **Add New...** button. The page "Add or Modify a Domain Filtering entry " will appear, shown in figure 5-36:

Add or Modify a Domain Filtering entry

Effective time: -

Domain Name:

Status:

Save Return

Figure 5-36 Add or Modify a Domain Filtering entry

To add or modify a Domain Filtering entry, follow these instructions:

1. **Effective Time** - Enter a range of time in HHMM format specifying the time for the entry to take effect. For example, if you enter: 0803 - 1705, then the entry will take effect from 08:03 to 17:05.
2. **Domain Name** - Type the domain or key word as desired in the field. A blank in the domain field means all websites on the Internet. For example: www.xxyy.com.cn, .net.
3. **Status** - Select **Enabled** or **Disabled** for this entry on the Status pull-down list.
4. Click the **Save** button to save this entry.

To modify or delete an existing entry:

1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enabled All** button to make all entries enabled.

Click the **Disabled All** button to make all entries disabled.

Click the **Delete All** button to delete all entries

Click the **Next** button to go to the next page and the **Previous** button to return to the previous page.

For example, if you want to block the PCs on your LAN to access websites www.xyy.com.cn, www.aabbcc.com and websites with .net in the end on the Internet while no limit for other websites, you should specify the following Domain filtering list:

ID	Effective time	Domain Name	Status	Modify
1	0000-2400	www.xyy.com	Enabled	Modify Delete
2	0800-2000	www.aabbcc.com	Enabled	Modify Delete
3	0000-2400	.net	Enabled	Modify Delete

5.8.4 MAC Filtering

Like the IP Address Filtering page, the MAC Address Filtering page (shown in figure 5-37) allows you to control access to the Internet by users on your local network based on their MAC Address.

MAC Address Filtering

Firewall Settings (You can change it on Firewall page)

Enable Firewall: **Enabled**

Enable MAC Address Filtering: **Disabled**

Default Filtering Rules: **Deny these PCs with enabled rules to access the Internet**

ID	MAC Address	Description	Status	Modify
<input type="button" value="Add New..."/> <input type="button" value="Enable All"/> <input type="button" value="Disable All"/> <input type="button" value="Delete All"/>				

Figure 5-37 MAC address Filtering

Before setting up MAC Filtering entries, you must ensure that **Enable Firewall** and **Enable MAC Filtering** have been selected on the Firewall page. To Add a MAC Address filtering entry, clicking the **Add New...** button. The page “Add or Modify a MAC Address Filtering entry” will appear, shown in figure 5-38:

Add or Modify a MAC Address Filtering Entry

MAC Address:

Description:

Status:

Figure 5-38 Add or Modify a MAC Address Filtering entry

To add or modify a MAC Address Filtering entry, follow these instructions:

1. Enter the appropriate MAC Address into the **MAC Address** field. The format of the MAC Address is XX-XX-XX-XX-XX (X is any hexadecimal digit). For example: 00-0E-AE-B0-00-0B.
2. Type the description of the PC in the **Description** field. For example: John's PC.
3. **Status** - Select **Enabled** or **Disabled** for this entry on the Status pull-down list.
4. Click the **Save** button to save this entry.

To add additional entries, repeat steps 1-4.

When finished, click the **Return** button to return to the MAC Address Filtering page.

To modify or delete an existing entry:

1. Click the **Modify** in the entry you want to modify. If you want to delete the entry, click the **Delete**.
2. Modify the information.
3. Click the **Save** button.

Click the **Enable All** button to make all entries enabled.

Click the **Disabled All** button to make all entries disabled.

Click the **Delete All** button to delete all entries

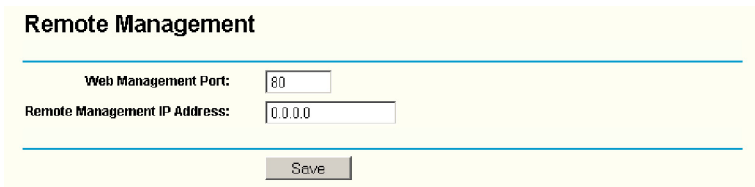
Click the **Next** button to go to the next page and click the **Previous** button to return to the previous page.

For example: If you want to block the PC with MAC addresses 00-0A-EB-00-07-BE and 00-0A-EB-00-07-5F to access the Internet, first, enable the **Firewall** and **MAC Address Filtering** on the **Firewall** page, then, you should specify the Default MAC Address Filtering Rule "**Deny these PCs with effective rules to access the Internet**" on the Firewall page and the following MAC address filtering list on this page:

ID	MAC Address	Description	Status	Modify
1	00-0A-EB-00-07-BE	John's computer	Enabled	Mcdify Delete
2	00-0A-EB-00-07-5F	Alice's computer	Enabled	Mcdify Delete

5.8.5 Remote Management

You can configure the Remote Management function on this page shown in figure 5-39. This feature allows you to manage your Router from a remote location, via the Internet.



Remote Management

Web Management Port:

Remote Management IP Address:

Figure 5-39 Remote Management

- **Web Management Port** - Web browser access normally uses the standard HTTP service port 80. This router's default remote management web port number is 80. For greater security, you can change the remote management web interface to a custom port by entering that number in this box provided. Choose a number between 1024 and 65534, but do not use the number of any common service port.
- **Remote Management IP Address** - This is the current address you will use when accessing your router from the Internet. The default IP Address is 0.0.0.0. It means this function is disabled. To enable this function, change the default IP Address to another IP Address as desired.

To access the router, you will type your router's WAN IP Address into your browser's Address (in IE) or Location (in Navigator) box, followed by a colon and the custom port number. For example, if your Router's WAN address is 202.96.12.8 and you use port number 8080, enter in your browser: `http://202.96.12.8:8080`. You will be asked for the router's password. After successfully entering the password, you will be able to access the router's web-based utility.

Note: Be sure to change the router's default password to a very secure password.

5.8.6 Advanced Security

Using Advanced Security page (shown in figure 5-40), you can protect the router from being attacked by TCP-SYN Flood, UDP Flood and ICMP-Flood from LAN.

Advanced Security

Packets Statistics Interval (5 ~ 60): 10 Seconds

DoS Protection: Disable Enable

Enable ICMP-FLOOD Attack Filtering
ICMP-FLOOD Packets Threshold (5 ~ 3600): 50 Packets/s

Enable UDP-FLOOD Filtering
UDP-FLOOD Packets Threshold (5 ~ 3600): 500 Packets/s

Enable TCP-SYN-FLOOD Attack Filtering
TCP-SYN-FLOOD Packets Threshold (5 ~ 3600): 50 Packets/s

Ignore Ping Packet From WAN Port
 Forbid Ping Packet From LAN Port

Figure 5-40 Advanced Security settings

- **Packets Statistic interval (5 ~ 60)** - The default value is 10. Select a value between 5 and 60 seconds in the pull-down list. The Packets Statistic interval value indicates the time section of the packets statistic. The result of the statistic used for analysis by SYN Flood, UDP Flood and ICMP-Flood.
- **DoS protection** - Enable or Disable the DoS protection function. Only when it is enabled, will the flood filters be effective.
- **Enable ICMP-FLOOD Attack Filtering** - Enable or Disable the ICMP-FLOOD Attack Filtering.
- **ICMP-FLOOD Packets threshold: (5 ~ 3600)** - The default value is 50. Enter a value between 5 ~ 3600 packets. When the current ICMP-FLOOD Packets numbers is beyond the set value, the router will start up the blocking function immediately.
- **Enable UDP-FLOOD Filtering** - Enable or Disable the UDP-FLOOD Filtering.
- **UDP-FLOOD Packets threshold: (5 ~ 3600)** - The default value is 500. Enter a value between 5 ~ 3600 packets. When the current UPD-FLOOD Packets numbers is beyond the set value, the router will start up the blocking function immediately.
- **Enable TCP-SYN-FLOOD Attack Filtering** - Enable or Disable the TCP-SYN- FLOOD Attack Filtering.
- **TCP-SYN-FLOOD Packets threshold: (5 ~ 3600)** - The default value is 50. Enter a value between 5 ~ 3600 packets. When the current TCP-SYN-FLOOD Packets numbers is beyond the set value, the router will start up the blocking function immediately.
- **Ignore Ping Packet from WAN Port** - Enable or Disable ignore ping packet from WAN port. The default is disabled. If enabled, the ping packet from the Internet cannot access the router.

Note: Please enable Current Statistics Status in System Tools > Statistics page to use the DOS Protection, refer to Chapter 5.11.8

- Forbid Ping Packet from LAN Port - Enable or Disable forbidding Ping Packet to access the router from the LAN port. The default value is disabled. If enabled, the ping packet from the LAN port cannot access the router. (Defends against some viruses)

Click the Save button to save the settings.

Click the Blocked DoS Host Table button to display the DoS host table by blocking. The page will appear that shown in figure 5-41:

Blocked Host List			
ID	Host IP Address	Host MAC Address	Modify
1	192.168.1.100	00-13-8F-AA-6D-77	Delete

Figure 5-41 Thwarted DoS Host Table

This page shows Host IP Address and Host MAC Address for each host blocked by the router.

- Host IP Address- The IP address that blocked by DoS are displayed here.
- Host MAC Address - The MAC address that blocked by DoS are displayed here.

To update this page and to show the current blocked host, click on the Refresh button.

Click the Clear All button to clear all displayed entries. After the table is empty the blocked host will regain the capability to access Internet.

Click the Return button to return to the Advanced Security page

5.9 IP & MAC Binding Setting

- IP & MAC Binding
 - Binding Setting
 - ARP List

Figure 5-4- the IP & MAC Binding menu

There are two submenus under the IP & MAC Binding menu (shown in Figure 5-42): Binding Setting and ARP List. Click any of them, and you will be able to scan or configure the corresponding function. The detailed explanations for each submenu are provided below.

5.9.1 Binding Setting

This page displays the IP & MAC Binding Setting table; you can operate it in accord with your desire. (shown in Figure 5-43).

IP & MAC Binding Setting

ARP Binding: Disable Enable

ID	MAC Address	IP Address	Bind	Modify
1	00-E0-4C-00-07-BE	192.168.1.4	<input checked="" type="checkbox"/>	Edit Delete

 Page

Figure 5-43 IP & MAC Binding Setting

- **MAC Address** - The MAC address of the controlled computer in the LAN.
- **IP Address** - The assigned IP address of the controlled computer in the LAN.
- **Bind** - Whether or not enable the arp binding.
- **Modify** - Edit or delete item.

When you want to add or modify an IP & MAC Binding entry, you can click the Add New button or Modify button, and then you will go to the next page. This page is used for adding or modifying an IP & MAC Binding entry (shown in Figure 5-44).

IP & MAC Binding Setting

Bind:

MAC Address:

IP Address:

Figure 5-44 IP & MAC Binding Setting (Add & Modify)

To add IP & MAC Binding entries:

1. Click the Add New.. button.
2. Enter the MAC Address and IP Address.
3. Select the Bind checkbox.
4. Click the Save button to save it.

To modify or delete an existing entry:

1. Find the desired entry in the table.
2. Click Modify or Delete as desired on the Modify column.

To find an existing entry:

1. Click the Find button (shown in Figure 5-43).
2. Enter the MAC Address or IP Address.
3. Enter the Find button in the next page (shown in Figure 5-45).

Find IP & MAC Binding Entry

MAC Address:

IP Address:

ID	MAC Address	IP Address	Bind	Link
1	00-E0-4C-00-07-BE	192.168.1.4	<input checked="" type="checkbox"/>	Turn to this page

Figure 5-45 Find IP & MAC Binding Entry

Click the Enable All button to make all entries enabled.

Click the Delete All button to delete all entries.

5.9.2 ARP List

To manage the computer, you could observe the computers in the LAN by checking the relationship of MAC address and IP address on the ARP list, and you could configure the items on the ARP list also. This page displays the ARP List; it shows all the existing IP & MAC Binding entries (shown in Figure 5-46).

ARP List				
ID	MAC Address	IP Address	Status	Configure
1	00-E0-4C-00-07-BE	192.168.1.4	Bound	<input type="button" value="Load"/> <input type="button" value="Delete"/>
2	00-13-8F-AA-6D-77	192.168.1.161	UnBound	<input type="button" value="Load"/> <input type="button" value="Delete"/>

Figure 5-46 ARP List

- **MAC Address** - The MAC address of the controlled computer in the LAN.
- **IP Address** - The assigned IP address of the controlled computer in the LAN.
- **Status** - Enabled or Disabled of the MAC address and IP address binding.
- **Configure** - Load or delete item.
- **Load** - Load the item to the IP & MAC Binding list.
- **Delete** - Delete the item.

Click the Bind All button to bind all the current items, available after enable.

Click the Load All button to load all items to the IP & MAC Binding list.

Click the Refresh button to refresh all items.

Note: An item could not be loaded to the IP & MAC Binding list if the IP address of the item has been loaded before. Error warning will prompt as well. Likewise, "Load All" only loads the items without interference to the IP & MAC Binding list.

5.10 Static Routing

A static route is a pre-determined path that network information must travel to reach a specific host or network. To add or delete a route, work in the area under the Static Routing page (shown in figure 5-47).

ID	Destination IP Address	Subnet Mask	Default Gateway	Status	Modify
1	202.109.37.42	255.255.255.0	202.109.37.1	Disabled	Modify Delete

Figure 5-47 Static Routing

To add static routing entries:

1. Click the Add New button. (pop-up figure 5-48)
2. Enter the following data:
 - **Destination IP Address** - The Destination IP Address is the address of the network or host that you want to assign to a static route.
 - **Subnet Mask** - The Subnet Mask determines which portion of an IP Address is the network portion, and which portion is the host portion.
 - **Gateway** - This is the IP Address of the gateway device that allows for contact between the router and the network or host.
3. Select Enabled or Disabled for this entry on the Status pull-down list..
4. Click the Save button to save it.

Add or Modify a Static Route Entry

Destination IP Address:
Subnet Mask:
Default Gateway:
Status:

Figure 5-48 Add or Modify a Static Route Entry

To modify or delete an existing entry:

1. Click the Modify in the entry you want to modify. If you want to delete the entry, click the Delete.
2. Modify the information.
3. Click the Save button.

Click the Enable All button to make all entries enabled.

Click the Disabled All button to make all entries disabled.

Click the Delete All button to delete all entries

5.11 Dynamic DDNS

The router offers a Dynamic Domain Name System (DDNS) feature. DDNS lets you assign a fixed host and domain name to a dynamic Internet IP Address. It is useful when you are hosting your own website, FTP server, or other server behind the router. Before using this feature, you need to sign up for DDNS service providers such as www.dyndns.org, www.oray.net or www.comexe.cn. The Dynamic DNS client service provider will give you a password or key.

To set up for DDNS, follow these instructions:

5.11.1 Dyndns.org DDNS

If your selected dynamic DNS Service Provider is www.dyndns.org, the page will appear as shown in figure 5-49:

DDNS

Service Provider: Dyndns (www.dyndns.org) [Go to register...](#)

User Name:

Password:

Domain Name:

Enable DDNS

Connection Status: DDNS not launching!

Figure 5-49 Dyndns.org DDNS Settings

To set up for DDNS, follow these instructions:

1. Type the domain names your dynamic DNS service provider gave.
2. Type the User Name for your DDNS account.
3. Type the Password for your DDNS account.
4. Click on Enable DDNS.
5. Click the Login button to login to the DDNS service.
 - Connection Status -The status of the DDNS service connection is displayed here.

Click Logout to logout of the DDNS service.

5.11.2 Oray.net DDNS

If your selected dynamic DNS Service Provider is www.oray.net, the page will appear as shown in figure 5-50:

DDNS

Service Provider: Peanut-Hull (www.oray.net) [Go to register...](#)

User Name:

Password:

Enable DDNS

Connection Status: Disconnected!

Service Type: ---

Domain Name: ---

Login Logout

Save

Figure 5-50 Oray.net DDNS Settings

To set up for DDNS, follow these instructions:

1. Type the User Name for your DDNS account.
2. Type the Password for your DDNS account.
3. Click on Enable DDNS.
4. Click the Login button to login the DDNS service.
 - Connection Status - The status of the DDNS service connection is displayed here.
 - Domain Name - The domain names are displayed here.

Click Logout to logout the DDNS service.

5.11.3 Comexe.cn DDNS

If your selected dynamic DNS Service Provider is www.comexe.cn, the page will appear as shown in figure 5-51:

DDNS

Service Provider: Comexe (www.comexe.cn) [Go to register...](#)

Domain Name:

Domain Name:

Domain Name:

Domain Name:

Domain Name:

User Name:

Password:

Enable DDNS

Connection Status: Disconnected !

Figure 5-51 Comexe.cn DDNS Settings

To set up for DDNS, follow these instructions:

1. Type the domain names your dynamic DNS service provider gave.
 2. Type the User Name for your DDNS account.
 3. Type the Password for your DDNS account.
 4. Click on Enable DDNS.
 5. Click the Login button to login to the DDNS service.
 - Connection Status -The status of the DDNS service connection is displayed here.
- Click Logout to logout of the DDNS service.

5.12 System Tools

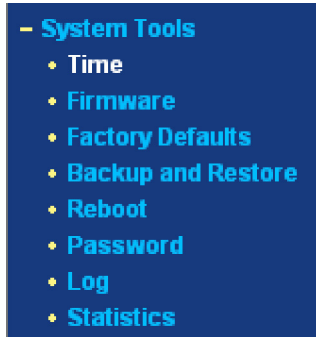


Figure 5-52 The System Tools menu

There are eight submenus under the System Tools menu (shown in figure 5-52): Time, Firmware, Factory Defaults, Backup and Restore, Reboot, Password, Log and Statistics. Click any of them, and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided.

5.12.1 Time

You can set time manually or get GMT from the Internet for the router on this page (shown in figure 5-53):

Time Settings

Time zone: (GMT+10:00) Brisbane, Canberra, Melbourne, Sydney ▾

Date: 1 1 2006 (MM/DD/YY)

Time: 9 22 44 (HH/MM/SS)

Using Daylight Saving Time:

DST begin : 0 0 0 (MM/DD/HH)

DST end: 0 0 0 (MM/DD/HH)

Preferable NTP Server: 0.0.0.0 0.0.0.0

(Get GMT when connected to Internet)

Figure 5-53 Time settings

- Time Zone - Select your local time zone from this pull down list.
- Date - Enter your local date in MM/DD/YY into the right blanks.
- Time - Enter your local time in HH/MM/SS into the right blanks.

Time setting follows these steps below:

1. Select your local time zone.
2. Enter date and time in the right blanks
3. Click Save.

Click the Get GMT button to get GMT time from Internet if you have connected to Internet.

If you're using Daylight saving time, please follow the steps below.

1. Select using daylight saving time.
2. Enter daylight saving beginning time and end time in the right blanks.
3. Click Save.

Note:

1. This setting will be used for some time-based functions such as firewall. You must specify your time zone once you login to the router successfully, if not, the time limited on these functions will not take effect.
2. The time will be lost if the router is turned off.
3. The router will obtain GMT automatically from Internet if it has already connected to Internet.

5.12.2 Firmware

The page (shown in figure 5-54) allows you to upgrade the latest version firmware to keep your router up-to-date.

Firmware

File: **Browse...**

Firmware Version: 3.5.3 Build 070511 Rel.30898n

Hardware Version: NetComm-NB504 v1.0 081520EF

Upgrade

Figure 5-54 Firmware Upgrade

New firmware is posted at www.netcomm.com.au and can be downloaded for free. If the router is not experiencing difficulties, there is no need to upgrade firmware, unless the new firmware supports a new feature you need.

Note: When you upgrade the router's firmware, you will lose current configuration settings, so make sure you backup the router's settings before you upgrade its firmware.

To upgrade the router's firmware, follow these instructions:

1. Download the latest firmware upgrade file from the Netcomm website (www.netcomm.com.au).
2. Click Browse to view the folders and select the downloaded file.
3. Click the Upgrade button.
 - Firmware Version - Displays the current firmware version.
 - Hardware Version - Displays the current hardware version. The hardware version of the upgrade file must accord with the current hardware version.

Note:

1. Do not turn off the router or press the Reset button while the firmware is being upgraded.
2. The router will reboot after the Upgrading has been finished.
3. Do not use wireless connection when updating firmware.
4. Turn off any firewall or anti-virus program

5.12.3 Factory Defaults

This page (shown in figure 5-55) allows you to restore the factory default settings for the router.

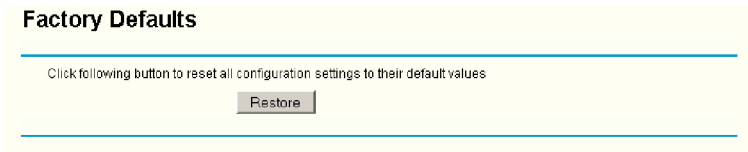


Figure 5-55 Restore Factory Default

Click the Restore button to reset all configuration settings to their default values.

- The default User Name: admin
- The default Password: admin
- The default IP Address: 192.168.1.1
- The default Subnet Mask: 255.255.255.0

Note: Any settings you have saved will be lost when the default settings are restored.

5.12.4 Backup and Restore

This page (shown in figure 5-56) allows you to save current configuration of router as backup or restore the configuration file you saved before.

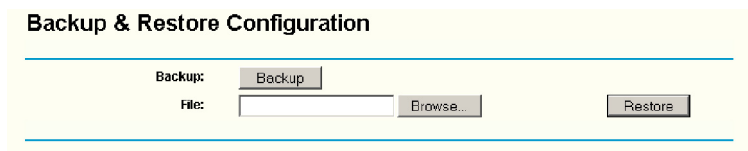


Figure 5-56 Backup & Restore Configuration

- Click the Backup button to save all configuration settings as a backup file in your local computer.
- To restore the router's configuration, follow these instructions:
- click the Browse button to select the backup file which you want to restore.
- Click the Restore button.

Note: The current configuration will be covered with the uploading configuration file. The restoration process lasts for 20 seconds and the router will restart automatically. Keep the router on during the restoring process, to prevent any damage.

5.12.5 Reboot

This page (shown in figure 5-57) allows you to reboot the router.

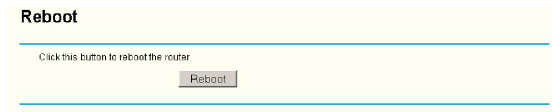


Figure 5-57 Reboot the router

Click the Reboot button to reboot the router.

Some settings of the router will take effect only after rebooting, which include:

- Change LAN IP Address. (System will reboot automatically)
- MAC Clone (system will reboot automatically)
- DHCP service function.
- Static address assignment of DHCP server.
- Web Service Port of the router.
- Upgrade the firmware of the router (system will reboot automatically).
- Restore the router's settings to factory default (system will reboot automatically).

5.12.6 Password

This page (shown in figure 5-58) allows you to change the factory default user name and password of the router.

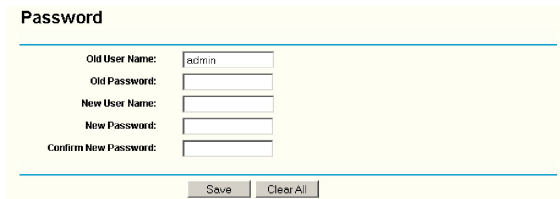


Figure 5-58 Password

It is recommended strongly that you change the factory default user name and password of the router. All users who try to access the router's web-based utility or Quick Setup will be prompted for the router's user name and password.

Note: The new user name and password must not exceed 14 characters in length and must not include any spaces. Enter the new Password twice to confirm it.

Click the Save button when finished.

Click the Clear All button to clear all.

5.12.7 Log

This page (shown in figure 5-59) allows you to query the logs of the router.

Log

Index	Log
1	1779:System: Logs were cleared.

Time = 2006-01-01 8:29:39 1779s

H-Ver = NetComm-NB504 v1.0 081520EF : S-Ver = 3.5.3 Build 070511 Rel.30898n

L = 192.168.1.1 : M = 255.255.255.0

W1 = DHCP : W = 0.0.0.0 : M = 0.0.0.0 : G = 0.0.0.0

Free=3097, Busy=1, Bind=0, Inv=0/0, Bc=0/4, Dns=0, cl=96, fc=0/0, sq=0/0

Figure 5-59 System Log

The router can keep logs of all traffic. You can query the logs to find what happened to the router.

Click the Refresh button to refresh the logs.

Click the Clear Log button to clear all the logs.

5.12.8 Statistics

The Statistics page (shown in figure 5-60) displays the network traffic of each PC in LAN, including total traffic and traffic of the last Packets Statistic interval seconds.

Statistics

Current Statistics Status: **Enabled**

Packets Statistics Interval(5-60): Seconds

Auto-refresh

Sorted Rules:

IP Address/ MAC Address	Total		Current				Modify	
	Packets	Bytes	Packets	Bytes	ICMP Tx	UDP Tx		SYN Tx
192.168.1.100 00-13-8F-AA-8D-77	1	58	0	0	0/0	0/0	0/0	Reset Delete

Figure 5-60 Statistics

- Current Statistics Status - Enable or Disable. The default value is disabled. To enable, click the Enable button. If disabled, the function of DoS protection in Security settings will be ineffective.
- Packets Statistics Interval - The default value is 10. Select a value between 5 and 60 seconds in the pull-down list. The Packets Statistic interval indicates the time section of the packets statistic.
- Sorted Rules - Select sorted rule of statistics results as your desired.

Statistics Table:

IP Address	The IP Address displayed with statistics	
Total	Packets	The total amount of packets received and transmitted by the router.
	Bytes	The total amount of bytes received and transmitted by the router.
Current	Packets	The total amount of packets received and transmitted in the last Packets Statistic interval seconds.
	Bytes	The total amount of bytes received and transmitted in the last Packets Statistic interval seconds.
	ICMP Tx	The total amount of the ICMP packets transmitted to WAN in the last Packets Statistic interval seconds.
	UDP Tx	The total amount of the UDP packets transmitted to WAN in the last Packets Statistic interval seconds.
	TCP SYN Tx	The total amount of the TCP SYN packets transmitted to WAN in the last Packets Statistic interval seconds.

Click the Save button to save the Packets Statistic interval value.

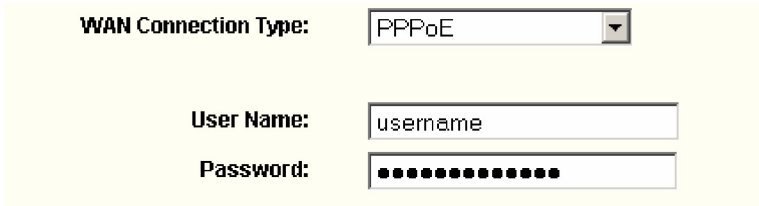
Click the Auto-refresh checkbox to refresh automatically.

Click the Refresh button to refresh immediately.

APPENDIX A: FAQ

1. How do I configure the router to access Internet by ADSL users?

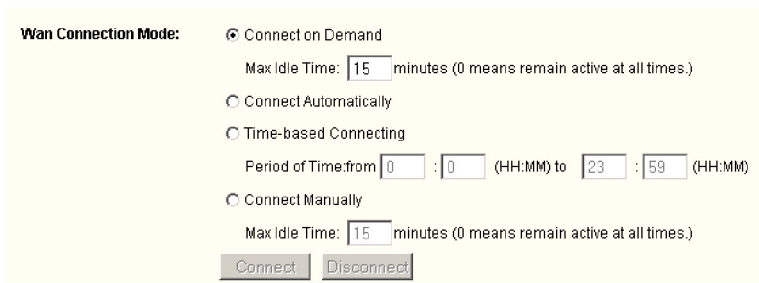
- 1) First, configure the ADSL modem configured in RFC1483 bridge model.
- 2) Connect the Ethernet cable from your ADSL modem to the WAN port on the router. The telephone cord plugs into the Line port of the ADSL modem.
- 3) Login to the router, click the “Network” menu on the left of your browser, and click “WAN” submenu. On the WAN page, select “PPPoE” for WAN Connection Type. Type user name in the “User Name” field and password in the “Password” field, finish by clicking “Connect”.



The screenshot shows the WAN configuration interface. The 'WAN Connection Type' is set to 'PPPoE' in a dropdown menu. Below it, the 'User Name' field contains 'username' and the 'Password' field is filled with 15 dots.

Figure A-1 PPPoE Connection Type

- 4) If your ADSL lease is in “pay-according-time” mode, select “Connect on Demand” or “Connect Manually” for Internet connection mode. Type an appropriate number for “Max Idle Time” to avoid wasting paid time. Otherwise, you can select “Auto-connecting” for Internet connection mode.



The screenshot shows the WAN Connection Mode configuration. The 'Wan Connection Mode' is set to 'Connect on Demand' (indicated by a checked radio button). The 'Max Idle Time' is set to 15 minutes. Other options include 'Connect Automatically', 'Time-based Connecting' (with a period of time from 0:00 to 23:59), and 'Connect Manually' (with a 'Max Idle Time' of 15 minutes). 'Connect' and 'Disconnect' buttons are visible at the bottom.

Figure A-2 PPPoE Connection Mode

Note:

- i. Sometimes the connection cannot be disconnected although you specify a time to Max Idle Time, since some applications is visiting the Internet continually in the background.
- ii. If you are a Cable user, please configure the router following the above steps.

2. How do I configure the router to access Internet by Ethernet users?

- 1) Login to the router, click the "Network" menu on the left of your browser, and click "WAN" submenu. On the WAN page, select "Dynamic IP" for "WAN Connection Type", finish by clicking "Save".
- 2) Some ISPs require that you register the MAC Address of your adapter, which is connected to your cable or DSL modem during installation. If your ISP requires MAC register, login to the router and click the "Network" menu link on the left of your browser, and then click "MAC Clone" submenu link. On the "MAC Clone" page, if your PC's MAC address is proper MAC address, click the "Clone MAC Address" button and your PC's MAC address will fill in the "WAN MAC Address" field. Or else, type the MAC Address into the "WAN MAC Address" field. The format for the MAC Address is XX-XX-XX-XX-XX-XX. Then click the "Save" button. It will take effect after rebooting.

MAC Clone

WAN MAC Address:	<input type="text" value="00-0A-EB-00-23-12"/>	<input type="button" value="Restore Factory MAC"/>
Your PC's MAC Address:	<input type="text" value="00-13-8F-AA-6D-77"/>	<input type="button" value="Clone MAC Address"/>

Figure A-3 MAC Clone

3. I want to use Netmeeting, what do I need to do?

- 1) If you start Netmeeting as a sponsor, you don't need to do anything with the router.
- 2) If you start as a responder, you need configure Virtual Server or DMZ Host.
- 3) How to configure Virtual Server: Login to the router, click the "Forwarding" menu on the left of your browser, and click "Virtual Servers" submenu. On the "Virtual Server" page, click Add New, then on the "Add or Modify a Virtual Server" page, enter "1720" into the blank behind the "Service Port", and your IP address behind the IP Address, assuming 192.168.1.169 for an example, remember to "Enable" and "Save".

Virtual Servers

ID	Service Port	IP Address	Protocol	Status	Modify
<input type="button" value="Add New.."/>	<input type="button" value="Enable All"/>	<input type="button" value="Disable All"/>	<input type="button" value="Delete All"/>		
<input type="button" value="Previous"/> <input type="button" value="Next"/>					

Figure A-4 Virtual Servers

Add or Modify a Virtual Server Entry

Service Port:	<input type="text" value="1720"/>	<input type="button" value="00000000"/>
IP Address:	<input type="text" value="192.168.1.169"/>	
Protocol:	<input type="text" value="ALL"/>	<input type="button" value="v"/>
Status:	<input type="text" value="Enabled"/>	<input type="button" value="v"/>
Common Service Port:	<input type="text" value="--Select One--"/>	
<input type="button" value="Save"/> <input type="button" value="Return"/>		

Figure A-5 Add or Modify a Virtual server Entry

Note: Your opposite side should call your WAN IP, which is displayed on the "Status" page.

- 4) How to enable DMZ Host: Login to the router, click the "Forwarding" menu on the left of your browser, and click "DMZ" submenu. On the "DMZ" page, click "Enable" radio and type your IP address into the "DMZ Host IP Address" field, using 192.168.1.169 as an example, remember to click the "Save" button

DMZ

Current DMZ Status:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
DMZ Host IP Address:	<input type="text" value="0.0.0.0"/>
<input type="button" value="Save"/>	

Figure A-6 DMZ

4. I want to build a WEB Server on the LAN, what should I do?

- 1) Because the WEB Server port 80 will interfere with the WEB management port 80 on the router, you must change the WEB management port number to avoid interference.
- 2) To change the WEB management port number: Login to the router, click the "Security" menu on the left of your browser, and click "Remote Management" submenu. On the "Remote Management" page, type a port number except 80, such as 88, into the "Web Management Port" field. Click "Save" and reboot the router.

Remote Management

Web Management Port:

Remote Management IP Address:

Figure A-7 Remote Management

Note: If the above configuration takes effect, to configure to the router by typing `http://192.168.1.1:88` (the router's LAN IP address: Web Management Port) in the address field of the web browser.

- 3) Login to the router, click the "Forwarding" menu on the left of your browser, and click the "Virtual Servers" submenu. On the "Virtual Server" page, click Add New, then on the "Add or Modify a Virtual Server" page, enter "80" into the blank behind the "Service Port", and your IP address behind the IP Address, assuming 192.168.1.188 for an example, remember to "Enable" and "Save".

Virtual Servers

ID	Service Port	IP Address	Protocol	Status	Modify
<input type="button" value="Add New"/>	<input type="button" value="Enable All"/>	<input type="button" value="Disable All"/>	<input type="button" value="Delete All"/>		

Figure A-8 Virtual Servers

Add or Modify a Virtual Server Entry

Service Port: 00-XX or XX

IP Address:

Protocol:

Status:

Common Service Port:

Figure A-9 Add or Modify a Virtual server Entry

5. The wireless stations cannot connect to the router.

- 1) Make sure the “Wireless Router Radio” is enabled.
- 2) Make sure that the wireless stations' SSID accord with the router's SSID.
- 3) Make sure the wireless stations have right KEY for encryption when the router is encrypted.
- 4) If the wireless connection is ready, but you can't access the router, check the IP Address of your wireless stations.

APPENDIX B: CONFIGURING THE PC

In this section, we'll introduce how to install and configure the TCP/IP correctly in Windows 95/98. First make sure your Ethernet Adapter is working, refer to the adapter's manual if needed.

1. Install TCP/IP component (if you use Windows 2000 or later, you can skip this step.)

- 1) On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
- 2) Double-click the Network icon, click on the Configuration tab in the appearing Network window.
- 3) Click on the Add button. Select Protocol, and then click Add.

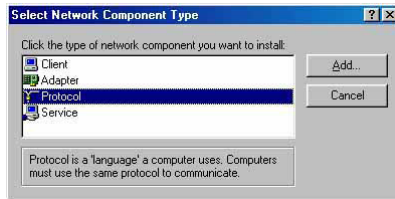


Figure B-1 Add Network Protocol

- 4) Under Manufacturers on Select Network Protocol page, highlight Microsoft. Under Network Protocols, highlight TCP/IP. Click OK. TCP/IP protocol will take effect after reboot.

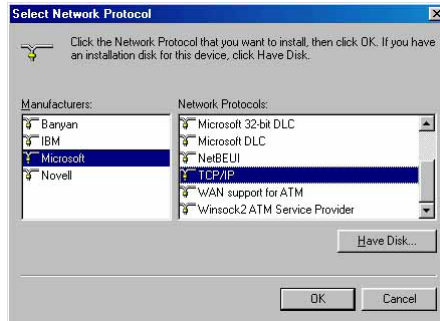


Figure B-2 Select Network Protocol

2. Configure TCP/IP for your computer

- 1) On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
- 2) Double-click the Network icon, highlight the bound TCP/IP tab in the appearing Network window that appears. An example is shown in the following figure:

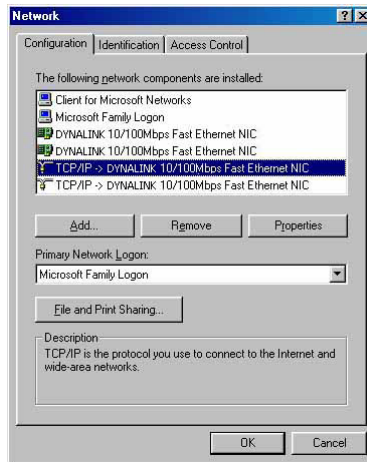


Figure B-3 Configuration tab

- 3) Click on Properties. The following TCP/IP Properties window will display and the IP Address tab is open on this window by default.
- 4) Now you have two ways to configure the TCP/IP protocol below:
 - Assigned by DHCP Sever
 - a. Select Obtain an IP address automatically, as shown in the figure below:

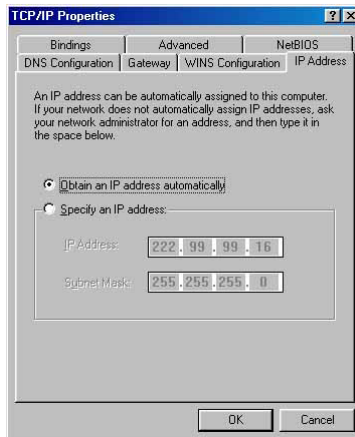


Figure B-4 IP Address tab

- b. Do not type anything into the New gateway field on the Gateway tab.

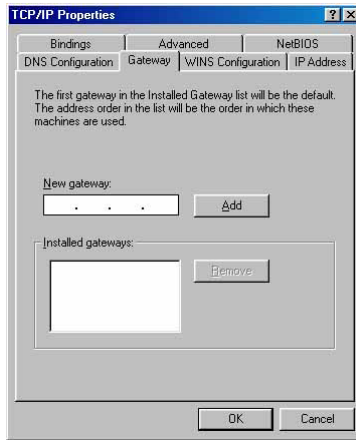


Figure B-5 Gateway tab

- c. Choose Disable DNS on the DNS configuration tab, as shown in the following figure:

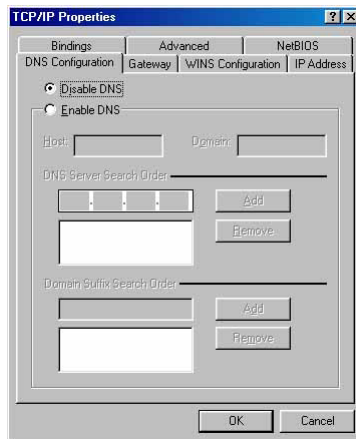


Figure B-6 DNS Configuration tab

- Setting IP address manually
 - a.

Select Specify an IP address on IP Address tab, as shown in the following figure. If the router's LAN IP address is 192.168.1.1, type IP address is 192.168.1.x (x is from 2 to 254), and subnet mask is 255.255.255.0.

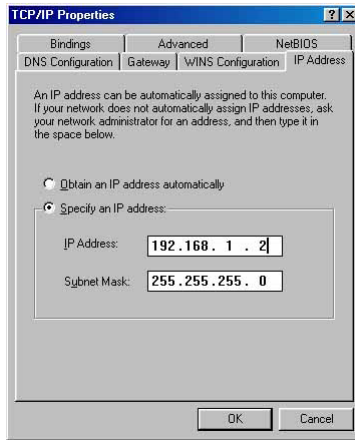


Figure B-7 IP Address tab

- b. Type the router's LAN IP address (the default IP is 192.168.1.1) into the New gateway field on the Gateway tab, and click on the Add button, as shown in the figure:

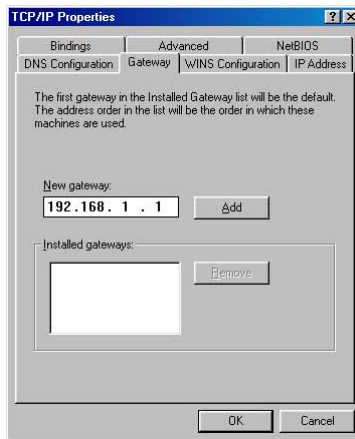


Figure B-8 Gateway tab

- c. On the DNS Configuration tab, click Enable DNS radio, and type your computer name in to the Host field and a Domain (such as szonline.com) into the Domain field. In the DNS Server Search Order field you can type the DNS server IP address, which has been provided by your ISP, and click Add button. Shown below:

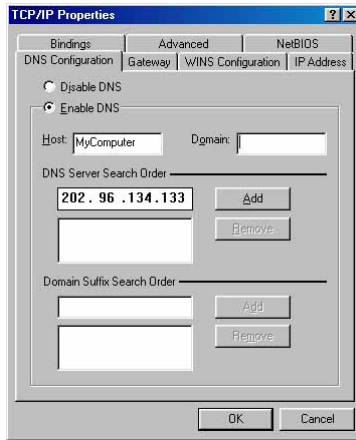


Figure B-9 DNS Configuration tab

- The configuration is now finished and will take effect after rebooting.

APPENDIX C: SPECIFICATIONS

General	
Standards	IEEE 802.3, 802.3u, 802.11b and 802.11g
Protocols	TCP/IP, PPPoE, DHCP, ICMP, NAT, SNTP
Ports	One 10/100M Auto-Negotiation WAN RJ45 port, Four 10/100M Auto-Negotiation LAN RJ45 ports supporting Auto MDI/MDIX
Cabling Type	10BASE-T: UTP category 3, 4, 5 cable (maximum 100m) EIA/TIA-568 100 STP (maximum 100m) 100BASE-TX: UTP category 5, 5e cable (maximum 100m) EIA/TIA-568 100 STP (maximum 100m)
Radio Data Rate	54/48/36/24/18/12/9/6Mbps or 11/5.5/3/2/1Mbps
Power Supply	9V~ 0.8A
LEDs	Power, System, WLAN, WAN, 1-4
Safety & Emissions	FCC, CE
Environmental and Physical	
Operating Temp.	0oC~40oC (32oF~104oF)
Operating Humidity	10% - 95% RH, Non-condensing
Dimensions (WxDxH)	186x146x44 mm (without antenna)

APPENDIX D: GLOSSARY

- **802.11b** - The 802.11b standard specifies a wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz, and WEP encryption for security. 802.11b networks are also referred to as Wi-Fi networks.
- **802.11g** - specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology, using OFDM modulation and operating in the unlicensed radio spectrum at 2.4GHz, and backward compatibility with IEEE 802.11b devices, and WEP encryption for security.
- **DDNS (Dynamic Domain Name System)** - The capability of assigning a fixed host and domain name to a dynamic Internet IP Address.
- **DHCP (Dynamic Host Configuration Protocol)** - A protocol that automatically configure the TCP/IP parameters for the all the PCs that are connected to a DHCP server.
- **DMZ (Demilitarized Zone)** - A Demilitarized Zone allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing.
- **DNS (Domain Name System)** – An Internet Service that translates the names of websites into IP addresses.
- **Domain Name** - A descriptive name for an address or group of addresses on the Internet.
- **DoS (Denial of Service)** - A hacker attack designed to prevent your computer or network from operating or communicating.
- **DSL (Digital Subscriber Line)** - A technology that allows data to be sent or received over existing traditional phone lines.
- **ISP (Internet Service Provider)** - A company that provides access to the Internet.
- **MTU (Maximum Transmission Unit)** - The size in bytes of the largest packet that can be transmitted.
- **NAT (Network Address Translation)** - NAT technology translates IP addresses of a local area network to a different IP address for the Internet.
- **PPPoE (Point to Point Protocol over Ethernet)** - PPPoE is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.
- **SSID** - A Service Set Identification is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID. This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name.
- **WEP (Wired Equivalent Privacy)** - A data privacy mechanism based on a 64-bit or 128-bit or 152-bit shared key algorithm, as described in the IEEE 802.11 standard.
- **Wi-Fi** - A trade name for the 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see <http://www.wi-fi.net>), an industry standards group promoting interoperability among 802.11b devices.
- **WLAN (Wireless Local Area Network)** - A group of computers and associated devices communicate with each other wirelessly, which network serving users are limited in a local area.

APPENDIX E: LEGAL & REGULATORY INFORMATION

This manual is copyright. Apart from any fair dealing for the purposes of private study, research, criticism or review, as permitted under the Copyright Act, no part may be reproduced, stored in a retrieval system or transmitted in any form, by any means, be it electronic, mechanical, recording or otherwise, without the prior written permission of NetComm Limited. NetComm Limited accepts no liability or responsibility, for consequences arising from the use of this product.

NetComm Limited reserves the right to change the specifications and operating details of this product without notice.

NetComm is a registered trademark of NetComm Limited.

All other trademarks are acknowledged the property of their respective owners.

Customer Information

ACA (Australian Communications Authority) requires you to be aware of the following information and warnings:

- (1) This unit shall be connected to the Telecommunication Network through a line cord which meets the requirements of the ACA TS008 Standard.
- (2) This equipment has been tested and found to comply with the Standards for C-Tick and or A-Tick as set by the ACA . These standards are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio noise and, if not installed and used in accordance with the instructions detailed within this manual, may cause interference to radio communications. However, there is no guarantee that interference will not occur with the installation of this product in your home or office. If this equipment does cause some degree of interference to radio or television reception, which can be determined by turning the equipment off and on, we encourage the user to try to correct the interference by one or more of the following measures:
 - Change the direction or relocate the receiving antenna.
 - Increase the separation between this equipment and the receiver.
 - Connect the equipment to an alternate power outlet on a different power circuit from that to which the receiver/TV is connected.
 - Consult an experienced radio/TV technician for help.
- (3) The power supply that is provided with this unit is only intended for use with this product. Do not use this power supply with any other product or do not use any other power supply that is not approved for use with this product by NetComm. Failure to do so may cause damage to this product, fire or result in personal injury.

Product Warranty

The warranty is granted on the following conditions:

1. This warranty extends to the original purchaser (you) and is not transferable;
2. This warranty shall not apply to software programs, batteries, power supplies, cables or other accessories supplied in or with the product;
3. The customer complies with all of the terms of any relevant agreement with NetComm and any other reasonable requirements of NetComm including producing such evidence of purchase as NetComm may require;
4. The cost of transporting product to and from NetComm's nominated premises is your responsibility; and,
5. NetComm does not have any liability or responsibility under this warranty where any cost, loss, injury or damage of any kind, whether direct, indirect, consequential, incidental or otherwise arises out of events beyond NetComm's reasonable control. This includes but is not limited to: acts of God, war, riot, embargoes, acts of civil or military authorities, fire, floods, electricity outages, lightning, power surges, or shortages of materials or labour.
6. The customer is responsible for the security of their computer and network at all times. Security features may be disabled within the factory default settings. NetComm recommends that you enable these features to enhance your security.

The warranty is automatically voided if:

1. You, or someone else, use the product, or attempts to use it, other than as specified by NetComm;
2. The fault or defect in your product is the result of a voltage surge subjected to the product either by the way of power supply or communication line, whether caused by thunderstorm activity or any other cause(s);
3. The fault is the result of accidental damage or damage in transit, including but not limited to liquid spillage;
4. Your product has been used for any purposes other than that for which it is sold, or in any way other than in strict accordance with the user manual supplied;
5. Your product has been repaired or modified or attempted to be repaired or modified, other than by a qualified person at a service centre authorised by NetComm; and,
6. The serial number has been defaced or altered in any way or if the serial number plate has been removed.

Limitations of Warranty

The Trade Practices Act 1974 and corresponding State and Territory Fair Trading Acts or legalisation of another Government ("the relevant acts") in certain circumstances imply mandatory conditions and warranties which cannot be excluded. This warranty is in addition to and not in replacement for such conditions and warranties.

To the extent permitted by the Relevant Acts, in relation to your product and any other materials provided with the product ("the Goods") the liability of NetComm under the Relevant Acts is limited at the option of NetComm to:

- Replacement of the Goods; or
- Repair of the Goods; or
- Payment of the cost of replacing the Goods; or
- Payment of the cost of having the Goods repaired.

All NetComm ACN 002 490 486 products have a standard 12 months warranty from date of purchase. However some products have an extended warranty option (refer to packaging). To be eligible for the extended warranty you must supply the requested warranty information to NetComm within 30 days of the original purchase by registering on-line via the NetComm web site at

www.netcomm.com.au

Product Warranty

NetComm products have a standard 12 months warranty from date of purchase. However some products have an extended warranty option, via registering your product online at the NetComm website www.netcomm.com.au. Refer to the User Guide for complete product warranty conditions, limitations of warranty and other legal and regulatory information.

Contact Information

If you have any technical difficulties with your product, please do not hesitate to contact NetComm's Customer Support Department.

Email: support@netcomm.com.au

www.netcomm.com.au

Note: NetComm Technical Support for this product only covers the basic installation and features outlined in the Quick Start Guide. For further information regarding the advanced features of this product, please refer to the configuring sections in the User Guide or contact a Network Specialist.

NetComm[®]
www.netcomm.com.au

NetComm Limited ABN 85 002 490 486
PO Box 1200, Lane Cove NSW 2066 Australia
E – sales@netcomm.com.au W – www.netcomm.com.au